List of Projects for Research in Information Security (Monsoon 2022)

Project 1: Designing an access control protocol for IoT-based drone or UAV environment

Requirements:

- Need to Design an access control protocol.
- Informal Security analysis for the proposed scheme
- Compare the security features with other related schemes
- Compare the communication and computation cost.

Reference: Basudeb Bera, Ashok Kumar Das, and Anil Kumar Sutrala. "Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in Internet of Drones environment," in ***Computer Communications (Elsevier)***, Vol. 166, No. 15, pp. 91-109, 2021. (2021 SCI Impact Factor: 5.047)

Project 2: Blockchain implementation using hyperledger fabric

Requirements

- With the help of hyperledger fabric blokchain based simulation need to perform.
- Encrypted & non-encrypted realtime dataset eg. Traffic or medical data should be used.
- Need to perform the simulation minimum 10 and maximum 50 P2P cloud server nodes.
- Need to perform and put the graph for no. of transactions with no. of mined nodes.
- No. of block addition with time, no. of transactions per second, throughput etc.

Reference: https://www.hyperledger.org/use/fabric

Project 3: Implementation of access control protocol with the help of Signing and Encryption (COSE).

Requirements:

- Need to show the performance, complete computation time.
- Only drone to drove or Drove to GSS scheme.
- Need to implement the proposed scheme using COSE
- While implementing you can consider Drone 1 (Server 1) and Drone 2 (Server 2) or Drone (Server 1) and GSS (Server 2) to sent the COSE messages.

Reference: Basudeb Bera, Sourav Saha, Ashok Kumar Das, Neeraj Kumar, Pascal Lorenz, and Mamoun Alazab. "Blockchain-Envisioned Secure Data Delivery and Collection Scheme for 5G-Based IoT-Enabled Internet of Drones Environment," in ***IEEE Transactions on Vehicular Technology***, Vol. 69, No. 8, pp. 9097-9111, 2020, DOI: 10.1109/TVT.2020.3000576. (2020 SCI Impact Factor: 5.978)

https://pycose.readthedocs.io/en/latest/

https://www.rfc-editor.org/rfc/rfc8152

https://datatracker.ietf.org/group/cose/about/

Project 4: Blockchain implementation using hyperledger sawtooth

Requirements

- With the help of hyperledger sawtooth blokchain based simulation need to perform.
- Encrypted & non-encrypted real-time datasets, e.g., traffic or medical data should be used.
- Need to perform the simulation minimum of 10 nodes and maximum of 50 P2P nodes.
- Need to perform and put the graph for no. of transactions with no. of nodes.
- No. of blocks addition with time, no. of transactions with time, throughput etc.

Reference: https://www.hyperledger.org/use/sawtooth

Project 5: Implementation of access control protocol using MIRACL library and formal security validation using Scyther automated software tool

Requirements

- Show the ECC operations and total execution time of the proposed protocol.
- Show the security analysis and what are the attacks possible and that are resist using Scyther.

Reference: Basudeb Bera, Sourav Saha, Ashok Kumar Das, and Athanasios V. Vasilakos. "Designing Blockchain-Based Access Control Protocol in IoT-Enabled Smart-Grid System," in ***IEEE Internet of Things Journal***, Vol. 8, No. 7, pp. 5744-5761, April 2021, DOI: 10.1109/JIOT.2020.3030308. (2020 SCI Impact Factor: 9.471)

https://people.cispa.io/cas.cremers/scyther/

https://github.com/miracl/MIRACL

Project 6: Implementation of authentication scheme using PBC (Pairing-Based Cryptography) library C or JAVA (JPBC)

Requirements

- Create 2 servers, consider server 1 as Client C and Server 2 as Application Provider AP.
- Only access control between Client C Application Provider AP needs to be implemented.

Reference: Odelu, V., Saha, S., Prasath, R., Sadineni, L., Conti, M., & Jo, M. (2019). Efficient privacy preserving device authentication in WBANs for industrial e-health applications. ***Computers & Security (Elsevier)***, 83, 300-312.

Or

Bagga, P., Das, A. K., & Rodrigues, J. J. (2023). Bilinear pairing-based access control and key agreement scheme for smart transportation. **Cyber Security and Applications (Elsevier)**, 1, 100001.

https://crypto.stanford.edu/pbc/

http://gas.dia.unisa.it/projects/jpbc/#.YwyG_NJBxuQ

Project 7: Design of Post Quantum Lattice-Based Secure Framework using Aggregate Signature for IoT-enabled healthcare applications

Requirements

- A solution need to provide for post-quantum Lattice-Based Framework using Aggregate Signature.
- Blockchain-based framework is suggested. Also, experiment the proposed approach based on delay, throughput, complexity will highly appreciated.

Reference:

Saha, R., Kumar, G., Devgun, T., Buchanan, W., Thomas, R., Alazab, M., ... & Rodrigues, J. (2021). A Blockchain Framework in Post-Quantum Decentralization. IEEE Transactions on Services Computing.

Project 8: Design of Identity-Based Multi-Signature Scheme for Internet of Vehicles Environment

Requirements

- Identity-Based multi-signature scheme need to proposed.
- Security analysis and correctness proof should be present.

Reference:

-Srivastava, V., Debnath, S. K., Bera, B., Das, A. K., Park, Y., & Lorenz, P. (2022). Blockchain-Envisioned Provably Secure Multivariate Identity-Based Multi-Signature Scheme for Internet of Vehicles Environment. IEEE Transactions on Vehicular Technology.

-Zhang, J., & Mao, J. (2009). A novel identity-based multi-signcryption scheme. Computer Communications, 32(1), 14-18.

Project 9: Design of Blockchain-Based Proxy Re-Encryption for Secure Data Sharing

Requirements

- A blockchain-based proxy re-encryption scheme needs to design with its correctness proof.

Reference:

- Guo, H., Zhang, Z., Xu, J., An, N., & Lan, X. (2018). Accountable proxy re-encryption for secure data sharing. IEEE Transactions on Dependable and Secure Computing, 18(1), 145-159.

- Manzoor, A., Liyanage, M., Braeke, A., Kanhere, S. S., & Ylianttila, M. (2019, May). Blockchain based proxy re-encryption scheme for secure IoT data sharing. In 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 99-103). IEEE.

Project 10: Design of Secure Search over Encrypted Cloud Data

Requirements

- Need to design a scheme for secure search scheme over encrypted cloud data
- Security analysis should be provided.

Reference:

- Yin, H., Qin, Z., Zhang, J., Ou, L., & Li, K. (2017). Achieving secure, universal, and fine-grained query results verification for secure search scheme over encrypted cloud data. IEEE transactions on cloud computing, 9(1), 27-39.

- Guan, Z., Wang, N., Fan, X., Liu, X., Wu, L., & Wan, S. (2020). Achieving secure search over encrypted data for e-commerce: a blockchain approach. ACM Transactions on Internet Technology (TOIT), 21(1), 1-17.

Project 11: Design of Secure Multi-Keyword Search over Encrypted Blockchain-Based Cloud Data

Requirements

- A multi keyword fuzzy search scheme need to design.
- The scheme supports multiple keyword search without increasing the index or search complexity.

Reference:

-Gao, S., Chen, Y., Zhu, J., Sui, Z., Zhang, R., & Ma, X. (2022). BPMS: Blockchain-based Privacy-preserving Multi-keyword Search in Multi-owner Setting. IEEE Transactions on Cloud Computing.

-Wang, B., Yu, S., Lou, W., & Hou, Y. T. (2014, April). Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud. In IEEE INFOCOM 2014-IEEE conference on computer communications (pp. 2112-2120). IEEE.

Project 12: Design of Blockchain-Based Encrypted Image Storage and Search in Cloud Computing

Requirements

- Need to propose blockchain based encrypted image storage and search system.
- Implementation can be provided using Python, Solidity, and conduct performance evaluations on local Ethereum client.

Reference:

Li, Y., Ma, J., Miao, Y., Liu, X., & Jiang, Q. (2022). Blockchain-Based Encrypted Image Storage and Search in Cloud Computing. In International Conference on Database Systems for Advanced Applications (pp. 413-421). Springer, Cham.

Project 13: Design of Federated Intrusion Detection in Blockchain-Based Smart Transportation Systems

Requirements

- A federated intrusion detection system need to create (can use deep learning architecture) for detecting cyber-attacks in heterogeneous smart transportation systems.
- The reference paper can be use for implementation.

Reference:

Abdel-Basset, M., Moustafa, N., Hawash, H., Razzak, I., Sallam, K. M., & Elkomy, O. M. (2021). Federated intrusion detection in blockchain-based smart transportation systems. IEEE Transactions on Intelligent Transportation Systems, 23(3), 2523-2537.

Project 14: Design of intrusion detection system using blockchain framework

Requirements

- An intrusion detection system need to design using blockchain framework
- Hyperledger fabric and Hyperledger sawtooth can be used to implement system.

Reference:

Khonde, S. R., & Ulagamuthalvi, V. (2022). Hybrid intrusion detection system using blockchain framework. EURASIP Journal on Wireless Communications and Networking, 2022(1), 1-25.

Project 15: Design of AI/ML-enabled Big data analytics for IoT environment

Requirements

- An architecture with artificial intelligence needs to provide for IoT applications.
- The performance evaluation of the architecture needs to be provided.

Reference:

-Singh, S. K., Rathore, S., & Park, J. H. (2020). Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence. Future Generation Computer Systems, 110, 721-743.