

EN-LAKP: Lightweight Authentication and Key Agreement Protocol for Emerging Networks

G. Lakpathi

Assistant Professor, Guru Nanak Institute of Technology, CSE Department, Hyderabad

ABSTRACT: Emerging network technologies that will be developed and implemented in the next generation to enhance computing facilities are Wireless Sensor Networks (WSNs) and Software Defined Networking (SDN). Since micro-electromechanical system (MEMS) technology progress, WSNs become more and more popular since they offer realistic and affordable real-time monitoring options. As a result, as network traffic and the variety of sensor nodes rise, the SDN paradigm is being integrated into WSN to avoid a performance bottleneck with traditional network design. Since the sensor nodes are dispersed throughout a hostile environment and they communicate over a public channel, the information shared between entities is vulnerable to attack. The proposed protocol illustrates why it made sense to provide network administration and control responsibilities to centralized SDN controller nodes. We thus offer the Lightweight Authentication and Key Agreement Protocol (LAKP) for SDN-enabled WSNs to protect entity communication. Furthermore, we demonstrate that the suggested solution avoids known security vulnerabilities by doing both formal and informal security examinations using the Scyther tool and Burrows-Abadi-Needham (BAN) logic.

I. INTRODUCTION

Traffic engineering (TE) has always attracted much research attention. Traditional TE concentrated on IP routing protocols, routing optimization problems, overlaying in an IP network, etc. Most of these studies were conducted in traditional IP networks. With the advent of the software defined network (SDN), researchers began to focus on TE issues in the SDN, including traffic splitting and SDN protocol design. The SDN can help us achieve efficient network management, which can solve massive TE issues that are difficult to realize in traditional networks. However, the SDN faces great challenges, e.g., scalability issues that limit its application scope. In addition, segment routing (SR) has advantages in network structure that can help solve these problems in the SDN. Therefore, many scholars began to explore the possibility of combining the SDN with segment routing. Segment routing is a novel network architecture that has realized further control of SDN in recent years. SR can achieve compatibility with the SDN, and it has become an implementation solution to some TE problems in the SDN. SR can realize directional data transmission from the source node to the destination node. However, the control overhead in SR is also unlimited in many different scenarios, which will cause inefficient data transmission. Meanwhile, existing solutions ignore the problem of an overlarge packet header in SR. Therefore, a routing scheme must be explored to achieve load balancing and consider the limited packet length in SR. Control overhead has an important problem in TE. Appropriate schemes for controlling overhead can optimize network transmission performance. In recent years, with the development of new network paradigms, i.e., the SDN, SR, and blockchain, control overhead optimization has been used in different frameworks. However, control overhead optimization is neglected in the SDN and SR. An unlimited control overhead causes an overlarge SR packet length, and decreases data transmission efficiency. The length of an SR packet header increases as the routing length grows, which deteriorates the control overhead situation in SR. Researchers did not optimize network performance from the aspect of limited control overhead when solving the issue of bandwidth load balancing in SR.

II. LITERATURE REVIEW

Y. Xue, K. Xue, N. Gai, J. Hong, D. S. Wei, and P. Hong. 2020. In public cloud storage services, data are outsourced to semi-trusted cloud servers which are outside of data owners' trusted domain. To prevent untrustworthy service providers from accessing data owners' sensitive data, outsourced data are often encrypted. In this scenario, conducting access control over these data becomes a challenging issue. Attribute-based encryption (ABE) has been proved to be a powerful cryptographic tool to express access policies over attributes, which can provide a fine-grained, flexible, and secure access control over outsourced data. However, the existing ABE-based access control schemes do not support users to gain access permission by collaboration. In this paper, we explore a special attribute-based access control scenario where multiple users having different attribute sets can collaborate to gain access permission if the data owner allows their collaboration in the access policy. Meanwhile, the collaboration that is not designated in the access policy should be regarded as a collusion and the access request will be denied. We propose an attribute-based controlled collaborative access control scheme through designating translation nodes in the access structure. Security analysis shows that our proposed scheme can guarantee data confidentiality and has many other critical security properties. Extensive performance analysis shows that our proposed scheme is efficient in terms of storage and computation overhead.

C. Batini, C. Cappiello, C. Francalanci, and A. Maurino. 2009. The literature provides a wide range of techniques to assess and improve the quality of data. Due to the diversity and complexity of these techniques, research has recently focused on defining methodologies that help the selection, customization, and application of data quality assessment and improvement techniques. The goal of this article is to provide a systematic and comparative description of such methodologies. Methodologies are compared along several dimensions, including the methodological phases and steps, the strategies and techniques, the data quality dimensions, the types of data, and, finally, the types of information systems addressed by each methodology. The article concludes with a summary description of each methodology.

Liu, Li, and Qi. 2019. Based on the influence of block chain technology on information sharing among supply chain participants, mean-CVaR (conditional value at risk) is used to characterize retailers' risk aversion behavior, while a Stackelberg game is taken to study the optimal decision-making of manufacturers and retailers during decentralized and centralized decision-making processes. Finally, the mean-CVaR-based revenue-sharing contract is used to coordinate the supply chain and profit distribution. The research shows that, under the condition of decentralized decision-making, when the retailer's optimal order quantity is low, it is an increasing function of the weighted proportion and the risk aversion degree, while, when the retailer's optimal order quantity is high, it is an increasing function of the weighted proportion, and has nothing to do with the risk aversion degree. The manufacturer's block chain technology application degree is a reduction function of the weighted proportion. When the retailer's order quantity is low, the manufacturer's block chain technology application degree is a decreasing function of risk aversion, while, when the retailer's order quantity is high, the manufacturer's block chain technology application is independent of risk aversion. The profit of the supply chain system under centralized decision-making is higher than that of decentralized decision-making. The revenue sharing contract can achieve the coordination of the supply chain to the level of centralized decision-making. Through block chain technology, transaction costs among members of the supply chain can be reduced, information sharing can be realized, and the benefits of the supply chain can be improved. Finally, the specific numerical simulation is adopted to analyze the weighted proportion, risk aversion and the impact of blockchain technology on the supply chain, and verify the relevant conclusions.

M. Ul Hassan, M. H. Rehmani, and J. Chen. 2020. Modern smart homes are being equipped with certain renewable energy resources that can produce their own electric energy. From time to time, these smart homes or micro grids are also capable of supplying energy to other houses, buildings, or energy grid in the time of available self-produced renewable energy. Therefore, researches have been carried out to develop optimal trading strategies, and many recent technologies are also being used in combination with micro grids. One such technology is block chain, which works over decentralized distributed ledger. In this paper, we develop a block chain based approach for micro grid energy auction. To make this auction more secure and private, we use differential privacy technique, which ensures that no

adversary will be able to infer private information of any participant with confidence. Furthermore, to reduce computational complexity at every trading node, we use consortium block chain, in which selected nodes are given authority to add a new block in the block chain. Finally, we develop differentially private Energy Auction for block chain-based micro grid systems (DEAL). We compare DEAL with Vickrey-Clarke-Groves (VCG) auction scenario and experimental results demonstrates that DEAL outperforms VCG mechanism by maximizing sellers' revenue along with maintaining overall network benefit and social welfare.

G. M. Hastig and M. S. Sodhi. 2020. We seek to guide operations management (OM) research on the implementation of supply chain traceability systems by identifying business requirements and the factors critical to successful implementation. We first motivate the need for implementing traceability systems in two very different industries—cobalt mining and pharmaceuticals—and present business requirements and critical success factors for implementation. Next, we describe how we carried out thematic analysis of practitioner and scholarly articles on implementing block chain for supply chain traceability. Finally, we present our results pertaining to the needs of different stakeholders such as suppliers, consumers, and regulators. The business requirements for traceability systems are curbing illegal practices; improving sustainability performance; increasing operational efficiency; enhancing supply-chain coordination; and sensing market trends. Critical success factors for implementation are companies' capabilities; collaboration; technology maturity; supply chain practices; leadership; and governance of the traceability efforts. These findings provide a nascent measurement model for empirical work and a foundation for descriptive and normative research on block chain applications for supply chain traceability.

D. Ivanov, A. Dolgui, and B. Sokolov. 2019. The impact of digitalization and Industry 4.0 on the ripple effect and disruption risk control analytics in the supply chain (SC) is studied. The research framework combines the results from two isolated areas, i.e. the impact of digitalization on SC management (SCM) and the impact of SCM on the ripple effect control. To the best of our knowledge, this is the first study that connects business, information, engineering and analytics perspectives on digitalization and SC risks. This paper does not pretend to be encyclopedic, but rather analyses recent literature and case-studies seeking to bring the discussion further with the help of a conceptual framework for researching the relationships between digitalization and SC disruptions risks. In addition, it emerges with an SC risk analytics framework. It analyses perspectives and future transformations that can be expected in transition towards cyber-physical SCs. With these two frameworks, this study contributes to the literature by answering the questions of (1) What relations exist between big data analytics, Industry 4.0, additive manufacturing, advanced trace & tracking systems and SC disruption risks? (2) How digitalization can contribute to enhancing ripple effect control; and (3) What digital technology-based extensions can trigger the developments towards SC risk analytics?

III. METHODOLOGY

We assume that the data owner is trusted, and the data users are authorized by the data owner. The communication channels between the owner and users are secure on existing security protocols such as SSL, TLS. With regard to the cloud server, our scheme resists a more challenging security model which is beyond the “semi-honest server” used in other secure semantic searching schemes. In our model, the dishonest cloud server attempts to return wrong/forged search results and learn sensitive information, but would not maliciously delete or tamper with the outsourced documents. Therefore, our secure semantic scheme should guarantee the verifiability, and confidentiality under such a security model.

Existing System Disadvantages

- a. Collection of quality characteristic data, high-speed safe transmission.
- b. Next-generation information technology.

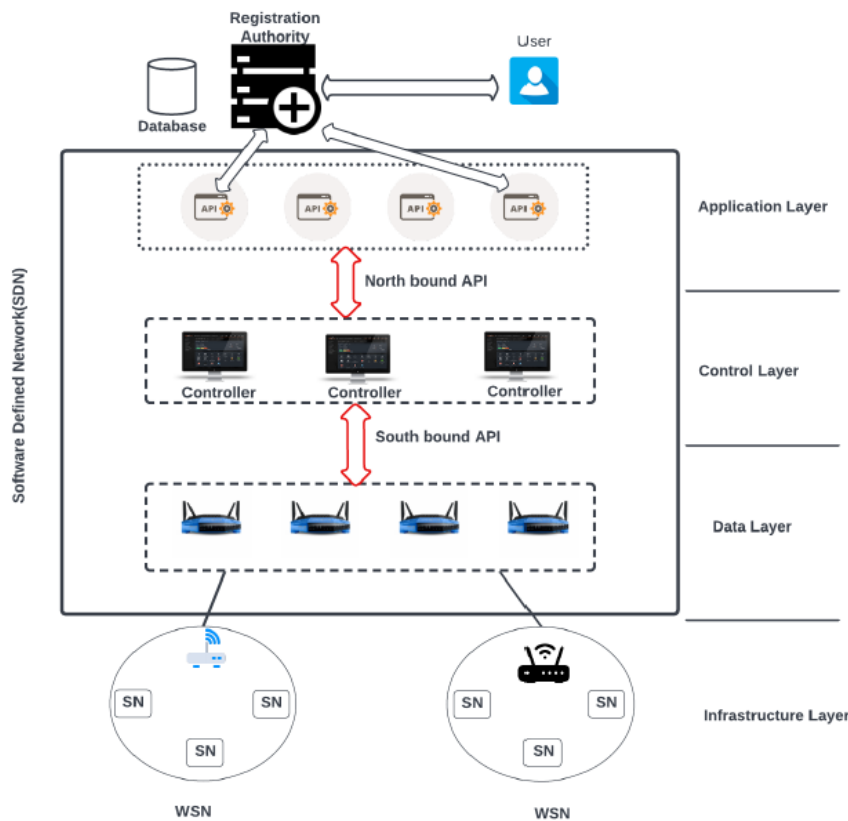
PROPOSED SYSTEM:

The proposed protocol showed how centralized SDN controller nodes logically assumed the role of network management and control. Therefore, we present a Lightweight Authentication and Key Agreement Protocol (LAKP) for SDN-enabled WSNs to protect entity communication. Additionally, we demonstrate that the suggested system prevents known security flaws by conducting both informal and formal security studies using the Scyther tool and Burrows-Abadi- Needham (BAN) logic. Further, the performance study demonstrates that the suggested scheme performs better in computing and communication burdens than related protocols with 1.6% to 5.4% and 1.3% to 5.8%, respectively.

Proposed System Advantages

- Sharing platform's real-time and orderly operation.
- data storage security sharing, and supplier assessment models on this foundation
- providing practical and intelligent sharing solutions for airlines

SYSTEM ARCHITECTURE



In this project data owner has a register all details and then login. Data owner can be an upload a document. Data owner can have a send request to the data user. Data user can search a query with uploaded document. The file has also a download it will show an encryption format. Data user also a send a request to the cloud server. Cloud server can a login. It will accept a key approve. Cloud server can also see all the data information's.

MODULES:

- 1. User Interface Design:** In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server. If the user already exists directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.
- 2. SR Controller:** This is the first module Data User can register and Login. After login Data User have an option of searching the files as a file name. Data user can also have a download file it will show an encrypted data. Data user can also send a trapdoor request to the server. Server can accept the request and then data user can takes permissions from the owner then the file it will downloaded in plain text.
- 3. Segment Routing:** This is the Second module of this project. In this module Data Owner should register and Login. Data Owner will Uploads the files into the database. Data owner can also send request to the data user.
- 4. Control Overhead optimization:** This is the third module of this project. In this module Cloud Server can login. After login it will see all data owners' information. Cloud server can see all users' information. Cloud server can see an all stored data files. Cloud server can give keys request to the user. Cloud server can also see an attacker information of file.

IV. IMPLEMENTATION

The project utilizes Java for backend logic, ensuring efficient data processing and business logic implementation. JSP (JavaServer Pages) is employed for dynamic web page generation, seamlessly integrating Java code within HTML for interactive content. This combination of Java and JSP creates a scalable and maintainable web application, ensuring a smooth user experience with responsive features.

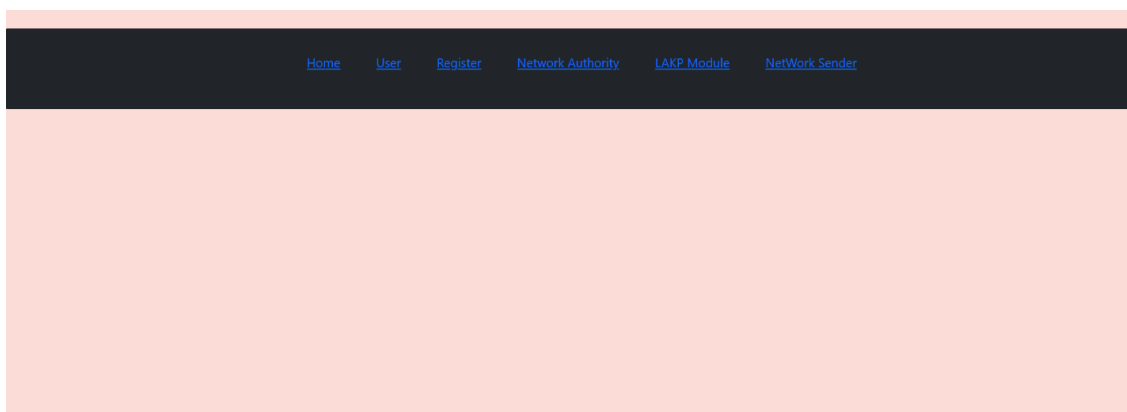

V. EXPERIMENTAL RESULTS

Fig: Index Page

REGISTER HERE



REGISTER

Fig: Data Owner Registration Page

CREATE NODE FOR CERTIFICATE

Mid	Service Chain	Certificate	Certificate Exchange	Create Node
6	Travel/Cityusertest1/Temp/20240409	d2fe44fe0fdb2936e697488f5cfc202db7078a6a13531886917a720eca3ff76	[[ID = 0; maximum queue length: 4], [ID = 1; maximum queue	Create Node

Fig: Data Sender Upload

CREATE KEY

Mid	Sender	Receiver	Message	Create Certificate
6	usertest1@gmail.com	test@gmail.com	sample test from usertest	Create Certificate

Fig: LAKP module Create Key

VI. CONCLUSION

Our investigation into authenticated key agreement protocols for the WSN environment revealed that most of them had either more performance requirements or were incapable of fulfilling the security requirements. Furthermore, the SDN paradigm has improved upon WSN to avoid a performance bottleneck with traditional network architecture as network traffic, and sensor nodes grow. Hence, we proposed a LAKP for emerging networks leveraging hash functions and XOR operations. Furthermore, the proposed protocol's security needs were assessed formally and informally using the Scyther tool and BAN logic. The proposed protocol protects against well-known attacks such as MIM, replay, impersonation, and insider attacks. The proposed protocol outperforms comparable protocols in terms of computation and communication burdens. The proposed protocol includes innovative features such as dynamic SN insertion and a user credential updating phase.

VII. FUTURE ENHANCEMENT

In the future, we plan to propose novel network framework for WSN environment and propose authentication protocol which mitigates physical and machine learning attacks.

1. Incorporation of Blockchain Technology: By incorporating blockchain technology, we can enhance the transparency and decentralization of the authentication process. Blockchain's immutable ledger can help prevent tampering and unauthorized access, ensuring the integrity of network communications.
2. Exploration of Post-Quantum Cryptography (PQC): PQC algorithms are designed to withstand attacks from quantum computers. Integrating PQC algorithms into LAKP can future-proof the protocol against advancements in quantum computing, ensuring long-term security for WSN environments.

REFERENCES

- [1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Comput. Netw.*, vol. 38, no. 4, pp. 393–422, 2002.
- [2] O. Gnawali, K.-Y. Jang, J. Paek, M. Vieira, R. Govindan, B. Greenstein, A. Joki, D. Estrin, and E. Kohler, "The Tenet architecture for tiered sensor networks," in *Proc. 4th Int. Conf. Embedded Networked Sensor Syst.*, Oct. 2006, pp. 153–166.
- [3] D. Yang, S. Misra, X. Fang, G. Xue, and J. Zhang, "Two-tiered constrained relay node placement in wireless sensor networks: Computational complexity and efficient approximations," *IEEE Trans. Mobile Comput.*, vol. 11, no. 8, pp. 1399–1411, Aug. 2012.
- [4] P. R. Babu, R. Amin, A. G. Reddy, A. K. Das, W. Susilo, and Y. Park, "Robust authentication protocol for dynamic charging system of electric vehicles," *IEEE Trans. Veh. Technol.*, vol. 70, no. 11, pp. 11338–11351, Nov. 2021.
- [5] H. Lu, D. Wang, Y. Li, J. Li, X. Li, H. Kim, S. Serikawa, and I. Humar, "CONet: A cognitive ocean network," *IEEE Wireless Commun.*, vol. 26, no. 3, pp. 90–96, Jun. 2019.
- [6] H. Lu, Y. Zhang, Y. Li, C. Jiang, and H. Abbas, "User-oriented virtual mobile network resource management for vehicle communications," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3521–3532, Jun. 2021.
- [7] Y. Zhang, Y. Li, R. Wang, M. S. Hossain, and H. Lu, "Multi-aspect aware session-based recommendation for intelligent transportation services," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4696–4705, Jul. 2021.