CONFIDENTIALITY PRESERVING CRYPTOGRAPIC CLARIFICATION FOR CLOUD STORAGE

ABSTRACT

In this thesis, we propose a novel equality test scheme aiming to solve the problem of equality test over ciphertext. Our scheme adopts the identity-based approach to make the solution more practical. To further ensure the integrity of cloud data, which can be first encrypted using our identity-based encryption with equality test, we propose cryptographic protocols suitable for the novel PAYG payment model to address the problems of data integrity checking in the cloud. The first protocol is time encapsulated that ensures the original file can be retrived after successful auditing by a client. The second protocol is a privacy-preserving public auditing protocol that allows a third-party auditor (TPA) to audit outsourced data on behalf of its clients without sacrificing the data or the timestamp (i.e., time of storage). We also suggest a data integrity checking scheme to simultaneously check the data content and storage duration represented by an updatable timestamp with strong privacy against TPA.

INTRODUCTION :

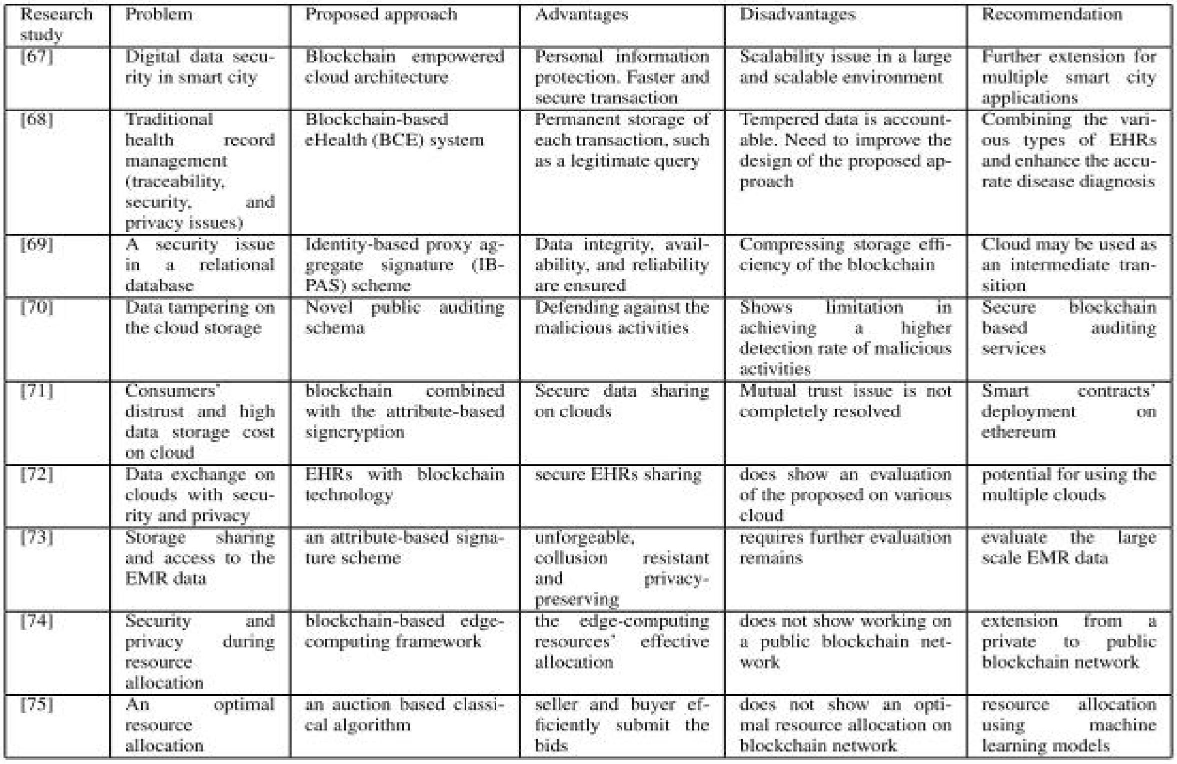
Cloud Computing concept has emerged from the distributed software architecture. Cloud computed technology is aimed to provide hosted services over the internet. In recent years, cloud computing in Information Technology has given rise to various new user communities and markets [1]. Cloud computing services are provided from data centers located in different parts of the world. Microsoft SharePoint and Google applications are general examples of cloud computing services.

Security plays an important role in the wider acceptance of cloud computing services [2]. Existing literature is focused on different security solutions, including technology and security policy implementation. The latter study introduced new attacks on the cloud environment from criminological perspectives. The proposed solution to these recent attacks s based on criminal theories for the protection of the cloud. A study [3] identified several security issues affecting cloud

computing attributes. The same research proposes to overcome the identified problems concerning the security of cloud. A security guide, developed in this research, enables the cloud user organizations to be aware of security vulnerabilities and approaches to invade them

The widely applied cloud has brought the rapid increase in digital data. In spite that the internet services are widely adopted in the daily life, cloud clients take a great concern to security and privacy of their digital data because of losing the direct control of their data managed by the cloud server. Security and privacy become significant barriers to the spread of various internet technologies, such as cloud computing and cloud storage. To protect the data privacy, cloud clients can upload their data in the encrypted form. However, this creates a barrier for data classification and search operations. Testing if two ciphertexts contain the same plaintext is a promising approach to address the problem.

BLOCKCHAIN BASED PROPSOED STUDIES :



Research study	Problem	Proposed approach	Advantages	Disadvantages	Recommendation
[67]	Digital data security in smart city	Blockchain empowered cloud architecture	Personal information protection. Faster and secure transaction	Scalability issue in a large and scalable environment	Further extension for multiple smart city applications
[68]	Traditional health record management (traceability, security, and privacy issues)	Blockchain-based eHealth (BCE) system	Permanent storage of each transaction, such as a legitimate query	Tempered data is accountable. Need to improve the design of the proposed approach	Combining the various types of EHRs and enhance the accurate disease diagnosis
[69]	A security issue in a relational database	Identity-based proxy aggregate signature (IB-PAS) scheme	Data integrity, availability, and reliability are ensured	Compressing storage efficiency of the blockchain	Cloud may be used as an intermediate transition
[70]	Data tampering on the cloud storage	Novel public auditing schema	Defending against the malicious activities	Shows limitation in achieving a higher detection rate of malicious activities	Secure blockchain based auditing services
[71]	Consumers' distrust and high data storage cost on cloud	blockchain combined with the attribute-based signcryption	Secure data sharing on clouds	Mutual trust issue is not completely resolved	Smart contracts' deployment on ethereum
[72]	Data exchange on clouds with security and privacy	EHRs with blockchain technology	secure EHRs sharing	does show an evaluation of the proposed on various cloud	potential for using the multiple clouds
[73]	Storage sharing and access to the EMR data	an attribute-based signature scheme	unforgeable, collusion resistant and privacy-preserving	requires further evaluation remains	evaluate the large scale EMR data
[74]	Security and privacy during resource allocation	blockchain-based edge-computing framework	the edge-computing resources' effective allocation	does not show working on a public blockchain network	extension from a private to public blockchain network
[75]	An optimal resource allocation	an auction based classical algorithm	seller and buyer efficiently submit the bids	does not show an optimal resource allocation on blockchain network	resource allocation using machine learning models

CONCLUSION AND FUTURE WORKS

First, in this SLR, we have reviewed the literature on cloud computing topics, including cloud security threats and their mitigation strategies. We identified several security risks to cloud computing. Data tampering and leakage is one of the identified risks. Consumers' trustworthiness, data outsourcing, and its associated risks are significant challenges identified in this SLR. This SLR identified commercial cloud services providers and highlighted the security issues they face during cloud services deployment and implementation.

The trustworthiness of cloud users is challenging to consumers of commercial cloud services providers. Data unavailability, insufficient security measures, and vendor lock-in, lack of interoperability and standards are identified additionally to above-mentioned issues. Moreover, we identified that Tweeter data generates and

is used to evaluate the proposed CC approaches. This SLR identified that researchers had rarely used Facebook and Instagram data for the evaluation of proposed strategies. During the CC deployment and implementations, data security and privacy are concerns that a cloud adopting must consider before using the cloud services. Blockchain technology isfound as an emerging technology to alleviate the security concerns in the CC environment. Cloud computing services have significant advantages for vendors and users but need to bridge security gaps for cloud users. Overall, this SLR claimed that security was the most critical issue for users and CSPs. Literature review supported our claim and thus it is suggested to propose an appropriate implementation of cloud computing security policies and standards. We have presented some recommendations in Table 4, which can be practiced, and implemented in future
works

REFERENCES :

[1] P. T. Jaeger, J. Lin, and J. M. Grimes, ‘‘Cloud computing and information policy: Computing in a policy cloud?’’ J. Inf. Technol. Politics, vol. 5, no. 3, Oct. 2008.

[2] C. Vidal and K.-K. R. Choo, ‘‘Situational crime prevention and the mitigation of cloud computing threats,’’ in Proc. Int. Conf. Secur. Privacy Commun. Syst. Springer, 2017.

[3] N. Khan and A. Al-Yasiri, ‘‘Cloud security threats and techniques to strengthen cloud computing adoption framework,’’ in Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications. Hershey, PA, USA: IGI Global, 2018

[4] H. A. Kholidy, A. Erradi, S. Abdelwahed, and F. Baiardi, ‘‘A risk mitigation approach for autonomous cloud intrusion response system,’’ Computing, vol. 98, no. 11, Nov. 2016.

[5] C.-J. Chung, P. Khatkar, T. Xing, J. Lee, and D. Huang, ‘‘NICE: Network intrusion detection and countermeasure selection in virtual network systems,’’ IEEE Trans. Dependable Secure Comput., vol. 10, no. 4, Jul. 2013.

[6] J.-Y. Park, S.-H. Na, and E.-N. Huh, ‘‘An optimal investment scheme based on ATM considering cloud security environment,’’ in Proc. 11th Int. Conf. Ubiquitous Inf. Manage. Commun., Jan. 2017.

[7] P. A. Boampong and L. A. Wahsheh, ‘‘Different facets of security in the cloud,’’ in Proc. 15th Commun. Netw. Simulation Symp., 2012.

[8] K. Jamsa, Cloud Computing: SaaS, PaaS, IaaS, Virtualization, Business Models, Mobile, Security and More. Burlington, MA, USA: Jones & Bartlett, 2012

[9] T. Dillon, C. Wu, and E. Chang, ‘‘Cloud computing: Issues and challenges,’’ in Proc. 24th IEEE Int. Conf. Adv. Inf. Netw. Appl., Apr. 2010

[10] A. Bouayad, A. Blilat, N. E. H. Mejhed, and M. El Ghazi, ‘‘Cloud computing: Security challenges,’’ in Proc. Colloq. Inf. Sci. Technol., Oct. 2012