**Summary of “RSPP: A Reliable, Searchable and Privacy-Preserving e-Healthcare System for Cloud-Assisted Body Area Networks”**

**Name:** Avineet Kumar Singh

**ID#:** M12135865

**Abstract.** The fast development of cloud computing and Internet of Things (IoT) has been reshaped from the conventional healthcare industry to a more ﬂexible and efﬁcient paradigm of e-healthcare. A group of wearable and/or implantable devices which forms a wireless body area network (BAN), gathers key vital signs (e.g., heart rate, blood pressure, temperature, pulse oxygen, etc.). These information’s are aggregated into a single ﬁle called personal health information (PHI) at an IoT gateway and then forwarded to a cloud server for storage. Third-party healthcare service providers (HSPs) can monitor patients’ PHI and provide timely diagnosis.This paradigm shift has raised a lot of security and privacy concerns of PHI.In this paper, authors have proposed a reliable, searchable and privacy-preserving e-healthcare system. The core of the system is a novel and full-ﬂedged dynamic SSE scheme.Searchable Symmetric Encryption (SSE), is considered more practical in terms of search efﬁciency for large datasets when compared to its public key-based counterpart.A dynamic SSE scheme with forward privacy is highly desirable.The proposed system is built upon a novel dynamic SSE scheme with forward privacy and delegated veriﬁability, which enables both patients and HSPs to conduct privacy-preserving search on the encrypted PHIs stored in the cloud and verify the correctness and completeness of retrieved search results simultaneously.The salient features such as forward privacy and delegated veriﬁability were achieved by a unique combination of the increasing counter, Bloom ﬁlter and aggregate MAC.The detailed security analysis as well as the extensive simulations on a large data set with millions of records demonstrated the practical efﬁciency of the proposed system for real world healthcare applications.

**Contributions.** The authors achieved remote patient monitoring in a secure and regulatory compliant manner via proposing a dedicated and efﬁcient dynamic SSE scheme for e-healthcare applications where PHIs are generated and stored in the cloud periodically compared to previously proposed SSE schemes which make trade-offs among security, search performance and storage overhead by exploring static and dynamic datasets. Previous SSE schemes mainly focused on general search applications on encrypted database clearly not suitable for our e-healthcare applications.

The authors also proposed an efﬁcient mechanism that provided patient-controlled search capability for HSPs, thereby extending the system to a multi-user setting, where the data owner and data user might be different.

**Weaknesses.** The weakness which were not addressed that the Secret key distribution were expensive and time consuming. It is required to be distributed to all members.

The repetitive updating of information could harm the Forward Secrecy (FS) as keyword association is very sensitive in medical environment.

.