ABSTRACT

In Supply Chain Management (SCM) system, products are moved from supplier to customer. It integrates and coordinates the flow of material and information from supplier to manufacturer, wholesaler, retailer and to consumer. Effective supply chain management system ensures the availability of product when needed. In this regard, Radio-Frequency IDentification (RFID) technology in the supply chain ensures that the right goods are available in the right place. RFID makes the supply chain considerably more precise and improves the efficiency and reliability of the entire chain. Business organizations are trying to overcome the supply chain bottlenecks by integrating the best technologies possible. In recent years, there has been an influx of cloud based SCM solutions hitting the market. Security is seen as a big challenge for cloud based SCM. This research work focuses on authentication issues in the various processes of cloud based SCM applications in which objects are tagged with an active RFID tag.

In this work, the existing RFID based security protocols are investigated and analyzed against known security vulnerabilities and also their performance with respect to the active RFID tag is evaluated. It is observed that many of the existing RFID protocols are computationally intensive. This motivated us to provide secure RFID authentication protocols with less computation in the RFID tag and without any trusted third party for cloud based SCM. The main objectives of this research work are to provide mutual authentication among the participating entities, to delegate the readers rights to another authenticated reader by eliminating reader-to-reader communication, to design an ownership transfer protocol in order to prevent counterfeiting products and to provide verifiability to the customer (not available in existing ownership

transfer protocol), and to design an object tracking protocol when the RFID tagged objects are in transit.

RFID is a valuable technology for tracking objects in the supply chain. Security and privacy requirements arise with the fast deployment of RFID in the supply chain in a heterogeneous environment. Authentication is one of the important security requirements in cloud based supply chain. There is a need for secure, efficient and scalable protocol for an agile supply chain. In the first work, an RFID authentication protocol with tag reader association is proposed and informal security analysis is carried out. Performance analysis is done with respect to the tag entity. The proposed protocol is scalable and it preserves tag/reader privacy, provides mutual authentication and is resistant to many attacks. Secrecy attack is prevented and proved by coding the proposed protocol using ProVerif tool, version 1.96. Comparison with the existing protocol in terms of communication cost shows that the proposed protocol outperforms the other protocols.

In SCM, tracking of a large object is made efficient by attaching multiple RFID tags in the object/product. In order to check the availability of an object, it is compulsory to ensure that all the parts are existing as well. The RFID tag can be interrogated by any reader deployed in the department. This approach enhances the object detection probability for each object but increases security and privacy risks. The communication between RFID readers and the tags in the same department is to be authenticated by preserving the privacy of both reader and the tag. Several researchers have developed variants of grouping protocol for authentication and for searching the tags. In the second work, recently proposed Shen et al.'s scheme for authenticating multiple tags in a group is analyzed. It is found that secret parameters are leaked and not applicable for dynamic inclusion of tags. An authentication protocol is proposed for communication between an object attached with multiple tags and

an RFID reader deployed in the department. The details about the object, its associated tags and the readers are stored in the cloud. Cloud storage provides scalability and anywhere anytime access. The communication between the reader and the cloud server is also authenticated. The proposed protocol is formally analyzed using GNY logic to prove mutual authentication. Informal analysis proves the efficiency of the proposed protocol against known attacks. The proposed protocol is also analyzed using automatic cryptographic protocol verifier tool ProVerif. In SCM, when objects move from one place/department to another, the same RFID readers are not used throughout the supply chain. So, current reader delegates its access right to the new reader. When an object is moved inside the organization, delegation takes place between the readers. Many of the existing delegation protocols use Trusted Third Party (TTP), which is practically difficult to incorporate or requires a keyed hash function or symmetric key encryption to be executed in the RFID tag, whereas tags cannot perform computationally intensive operations. Our third work aims to simplify the delegation process by removing the usage of a TTP as well as eliminating reader-to-reader communication which avoids fixing the reader sequence in advance. Also, it preserves the security and privacy requirements for cloud based SCM applications. The proposed protocol withstands many attacks like tracing attack, tag impersonation attack, reader impersonation attack and privacy attack. The proposed protocol not only resists the above-mentioned attacks but also achieves mutual authentication, anonymity property and forward/backward secrecy. The protocol is analyzed formally using GNY logic, which ensures that the protocol achieves mutual authentication. Performance analysis is carried out and it shows that the proposed protocol is relatively better than the existing related schemes with respect to tag computation and communication cost.

Most of the existing RFID based ownership transfer protocols are in need of TTP or require a reader-to-reader communication in a centralized system. In the post supply chain, the products are to be tracked to prove their

originality in a distributed environment. The fourth work in this thesis aims to provide a verifiable ownership transfer of products attached with an RFID tag using blockchain technology to address various security requirements. The proposed protocol consists of two phases; in the first phase the buyer commits to buy the product and in the second phase actual ownership is transferred from the seller to the buyer. An informal analysis of the proposed protocol is carried out and it shows that it is relatively better than the existing related schemes with respect to security requirements.

Object tracking is a fundamental problem in SCM. Recent innovations eliminate the difficulties in traditional approach such as manual counting, locating the object and data management. RFID is a major prerequisite for IoT, which connects physical objects to the Internet. Various research works have been carried out to perform object tracking using GPS, video cameras and WiFi technology. These methods just hope to see the actual object, but not the characteristic changes of the object due to the environmental changes. After reviewing the implementation of the latest technologies in the object tracking system, it is expected that the security and privacy risks in large-scale IoT systems are to be eliminated and efficient IoT services are to be provided to SCM applications. In the fifth work, an architecture is proposed for a fine-grained IoT-enabled online object tracking system. Cloud storage used in this architecture enhances the scalability and data management. A novel secure and efficient end to end authentication protocol that is based on a symmetric key cryptosystem and a one-way hash function is proposed. A new scheme is also proposed to address object tracking communication flow which uses the secret key established in the authentication process. Tag/Reader impersonation attack and replay attack are prevented in the proposed scheme. It also preserves forward and backward secrecy. Performance analysis shows that the proposed protocol is not storage and computationally intensive.