BIOMETRIC SMARTCARD AUTHENTICATION FOR FOG COMPUTING

Kashif Munir and Lawan A. Mohammed

University of Hafr Al Batin, KSA

ABSTRACT:

In the IoT scenario, things at the edge can create significantly large amounts of data. Fog Computing has recently emerged as the paradigm to address the needs of edge computing in the Internet of Things (IoT) and Industrial Internet of Things (IIoT) applications. In a Fog Computing environment, much of the processing would take place closer to the edge in a router device, rather than having to be transmitted to the Fog. Authentication is an important issue for the security of fog computing since services are offered to massive-scale end users by front fog nodes.Fog computing faces new security and privacy challenges besides those inherited from cloud computing. Authentication helps to ensure and confirms a user's identity. The existing traditional password authentication does not provide enough security for the data and there have been instances when the password-based authentication has been manipulated to gain access into the data. Since the conventional methods such as passwords do not serve the purpose of data security, research worksare focused on biometric user authentication in fog computing environment. In this paper, we present biometric smartcard authentication to protect the fog computing environment.

KEYWORDS:

Biometric Authentication, Fog Computing, Security

1. INTRODUCTION

Fog computing, also known as fogging/edge computing, is a model in which data, processing,and applications are concentrated in devices at the network edge rather than existing almost entirely in the fog as per Cisco [6]. The concentration means that data can be processed locally in smart devices rather than being sent to the fog for processing. As per [26], Fog computing is one approach to dealing with the demands of the ever-increasing number of Internet-connected devices sometimes referred to as IoT. Cisco recently delivered the vision of fog computing to run applications on connected devices that would run directly at the network edge. Customers can develop, manage, and run software applications on the Cisco framework of the networked devices. This includes the difficult routes and switches. Cisco brought this new innovation where they combined the open-source Linux and network operating system together in a single network device.

According to [3], fog computing is considered as an extension of the cloud computing to the edge of the network, which is a highly virtualized platform of the resource pool that provides computation, storage, and networking services to nearby end users. As per [23], fog computing as "*a scenario where a huge number of heterogeneous (wireless and sometimes autonomous) ubiquitous and decentralized devices communicate and potentially cooperate among them and with the network to perform storage and processing tasks without theintervention of third parties. These tasks can beused for supporting basic network functions or new services and applications*

that run in a sandboxed environment. Users leasing part of their devices to host these services get incentives for doing so." Although those definitions are still debatable before, fog computing is no longer a buzzword.

According to [4],Fog model provides benefits in advertising, computing, entertainment, and other applications, well positioned for data analytics and distributed data collection points. End services like, set-up-boxes and access points can be easily hosted using fogging. It improves QoS and reduces latency. The main task of fogging is positioning information near to the user at the network edge. In general, some of the major benefits of fog computing are:

- The significant reduction in data movement across the network resulting in reduced congestion, cost and latency, elimination of bottlenecks resulting from centralized computing systems, improved security of encrypted data as it stays closer to the end user reducing exposure to hostile elements and improved scalability arising from virtualized systems.
- Eliminates the core computing environment, thereby reducing a major block and a point of failure.
- Improves the security, as data are encoded as it is moved towards the network edge.
- Edge Computing, in addition to providingthe sub-second response to end users, it also provides high levels of scalability, reliability and fault tolerance.
- Consumes less amount of bandwidth.

The OpenFog consortium released the OpenFog reference architecture (RA) recommendations for anyone wishing to implement fog computing or any fog-based applications. The OpenFog Reference Architecture is based on eight core technical principles, termed pillars, which represent the key attributes that a system needs to encompass to be defined as "OpenFog." These pillars include security, scalability, openness, autonomy, RAS (reliability, availability, and serviceability), agility, hierarchy and programmability.

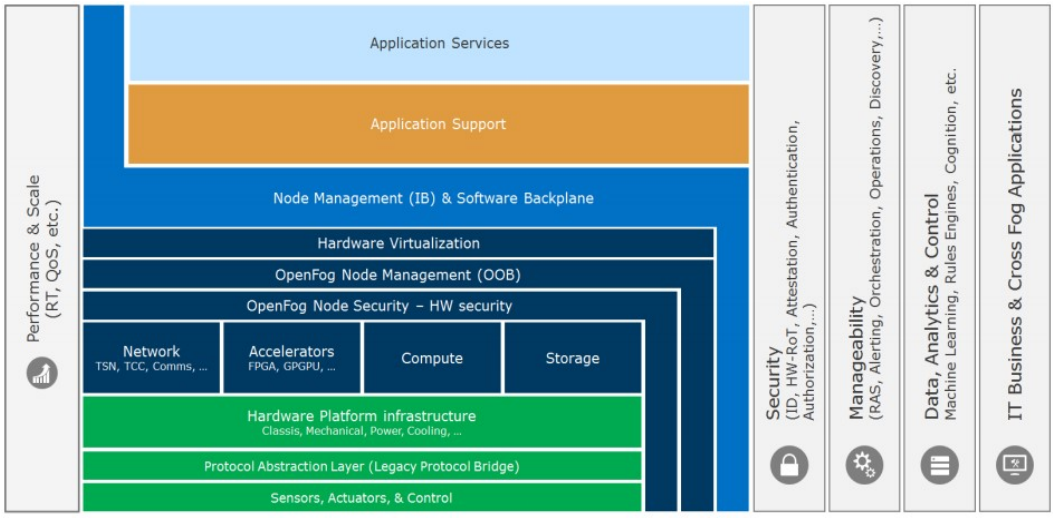

Figure 1: The OpenFog Reference Architecture(https://www.openfogconsortium.org/ra/)

A detailed architecture stack shows the interrelationships between various hardware, software infrastructure, and application software layers, as well as various cross-cutting concernssuchas

security, performance, manageability, analytics and controlthat impact the function of all layers. As security is one of the most complex and critical aspects of IoT systems, a special appendix dives deeply into OpenFog security guidelines. The OpenFog architecture is depicted in figure 1 above.

2. RELATED WORK

Although there are numerous novel studies contributed tothe secure authentication system, recent studies have mostly considered cloud storage environments rather than fog computing. In this section, we briefly summarize some few ones among those that address fog computing and point out their limitations and difficulties in direct adoption to the fog storage architecture.

Some authentication protocols which have been proposed for fog computing systems were described in many articles. However, only a few of them can achieve privacy preservation. The first type of such authentication protocols uses symmetric key encryption algorithmsdue to their low computational cost [11][21][22]. However, these protocols can be attacked by man-in-the-middle attacks, and the privacy information will inevitably be revealed. Another drawback of these protocols is the inherent scalability problem for privacy preservation, which makes them undoubtedly impractical. The second type of such authentication protocols updates an end-device's credentials regularly[13][24][25]. However, during the validity period of the credential, the strong identity of an end-device can still be tracked. Furthermore, such protocols require each end-device to store a large number of certifications and pseudonyms, which means that it is difficult to remove a compromised end-device. The third type of such authentication protocols uses a delegation-based mechanism [5]. The advantage is their low computational cost, but the disadvantage is that the privacy-preserving property cannot be easily achieved. To overcome this limitation, we proposed a three-factor authentication using both smart card and biometrics.

3. SECURITY CHALLENGES

In spite of the fact that Fog Computing can play a central role in delivering a rich portfolio of services more effectively and efficiently to end users, it could impose security and privacy challenges. The major security and privacy challenges in fog computing are summarized below.

TRUST MODEL.

Trust models based on reputation have been successfully deployed in many scenarios such as online social networks. Reputation-based trust model proposed by [10]has been successful in eCommerce, peer-to-peer (P2P), user reviews and online social networks.

Research conducted by[7], proposed a robust reputation system for resource selection in P2P networks using a distributed polling algorithm to assess the reliability of a resource before downloading. In designing a fog computing reputation-based reputation system, we may need to tackle issues such as

a) How to achieve persistent, unique, and distinct identity,
b) How to treat intentional and accidental misbehavior,
c) How to conduct punishment and redemption of reputation.

There are also trusting models based on special hardware such as Secure Element (SE), Trusted Execution Environment (TEE), or Trusted Platform Module (TPM), which can provide trust utility in fog computing applications[17].

Research conducted by[18], it wassuggestedthat to design a trust model based on reputation in the IoT, we need to tackle how to maintain the service reliability and prevent accidental failures, handle and identify misbehavior issues, identify malicious behavior correctly, and bootstrap building a trust model based on reputation in large-scale networks.

ROGUE FOG NODE

A rogue fog node would be a fog device or fog instance that pretends to be legitimate and coaxes end users to connect to it. For example, in an insider attack, a fog administrator may be authorized to manage fog instances, but may instantiate a rogue fog instance rather than a legitimate one. [20] have demonstrated the feasibility of man-in-the-middle attack in fog computing, before which the gateway should be either compromised or replaced by a fake one. Once connected, the adversary can manipulate the incoming and outgoing requests from end users or fog, collect or tamper user data stealthily, and easily launch further attacks.The existence of fake fog node will be a big threat to user data security and privacy. This problem is hard to address in fog computing due to several reasons

a) Complex trust situation calls for different trust management schemes,
b) Dynamic creating, deleting of virtual machine instance make it hard to maintain a blacklist of rogue nodes.

A rogue IoT node has the potential to misuse users' data or provides malicious data to neighboring nodes to disrupt their behaviors. Addressing this problem could be difficult in the IoT due to the complexity in trust management in various schemes. However, a trust measurement-based model could be applied to detect rogue nodes in IoT environments' which can provide limited security protection.

AUTHENTICATION

Authentication is an important issue for the security of fog computing since services are offered to massive-scale end users by front fog nodes. [20] have considered the main security issue of fog computing as the authentication at different levels of fog nodes. Traditional PKI-based authentication is not efficient and has poor scalability. [2] have proposed a cheap, secure and user-friendly solution to the authentication problem in local ad-hoc wireless network, relying on a physical contact for pre-authentication in a location-limited channel.

As the emergence of biometric authentication in mobile computing and fog computing, such as fingerprint authentication, face authentication, touch-based or keystroke-based authentication, etc., it will be beneficial to apply biometric-based authentication in fog computing.

ACCESS CONTROL

As per [1], Access control is a security technique to ensure that only authorized entities can access a certain resource, such as an IoT device, or the collected data. In the IoT, we need access control to make sure that only trusted parties can perform a given action such as accessing IoT device data, issuing a command to an IoT device, or updating IoT device software.

Research conducted by[9],propose a policy-based resource access control in fog computing, to support secure collaboration and interoperability between heterogeneous resources. In fog computing, how to design access control spanning client-fog-fog, at the same time meet the designing goals and resource constraints will be challenging.

INTRUSION DETECTION

As per [15],Intrusion detection techniques are widely deployed in fog system to mitigate attacks such as insider attack, flooding attack, port scanning, attacks on VM and hypervisor. In fog computing, Intrusion Detection System (IDS) can be deployed on fog node system side to detect intrusive behavior by monitoring and analyzing log file, access control policies and user login information. They can also be deployed at the fog network side to detect malicious attacks such as denial-of-service (DoS), port scanning, etc. In fog computing, it provides new opportunities to investigate how fog computing can help with intrusion detection on both client-side and the centralized fog side.

Research conducted by[19], a foglet mesh based security framework which can detection intrusion to distance fog, securing communication among mobile devices, foglet and fog. There are also challenges such as implementing intrusion detection in geo-distributed, large-scale, high-mobility fog computing environ men to meet the low-latency requirement.

4. BIOMETRIC SMARTCARD AUTHENTICATION FOR FOG COMPUTING SERVICES – A PROTOTYPE

Biometric identification is utilized to verify a person's identity by measuring digitally certain human characteristics and comparing those measurements with those that have been stored in a template for that same person. Details can be found in [10]. Templates can be stored at the biometric device, the institution's database, a user's smart card, or a *Trusted Third Party* service provider's database. There are two major categories of biometric techniques: *physiological* (fingerprint verification, iris analysis, hand geometry-vein patterns, ear recognition, odor detection, DNA pattern analysis and sweat pores analysis), and *behavioral* (handwritten signature verification, keystroke analysis and speech analysis) [16].Research conducted by[8], it was found that behavior-based systems were perceived as less acceptable than those based on physiological characteristics. Of the physiological techniques, the most commonly utilized is that of fingerprint scanning. With biometrics, fraudulent incidents can be minimized, as an added layer of authentication is now introduced that ensures that even with the correct pin information and in possession of another person's card, the user's biometric features cannot easily be faked. The advantages of this may include: all attributes of the cards will be maintained, counterfeiting attempts are reduced due to enrolment process that verifies identity and captures biometrics, and it will be extremely high security and excellent user-to-card authentication. These advantages are

for the benefit of users as well as system administrators because the problems and costs associated with lost, reissued or temporarily issued can be avoided, thus saving some costs of the system management.

On the negative side, the major risk posed by the use of biometric systems is that a malicious subject may interfere with the communication and intercept the biometric template and use it later to obtain access [14]. Likewise, an attack may be committed by generating a template from a fingerprint obtained from some surface. Although few biometric systems are fast and accurate in terms of low false acceptance rate enough to allow identification (automatically recognizing the user identity), most of the current systems are suitable for the verification only, as the false acceptance rate is too high.

The proposed design uses a maximum of 8 characters, numbers or mix of both PIN and fingerprint as verification factors of the authentication process. ACOS smartcards and AET60 BioCARDKey development kit were used in the proposed design. In the verification part, the users have to submit the correct PIN DES encrypted current session key to get access to the next level. Users have 3 successful attempts to enter the correct PIN, else the cards will be locked and render it to useless. Lastly, Authors use the fingerprint as the biometric identifiers as it takes shortest enrollment time. The proposed design involves two phases namely the enrollment phase and verification phase. Each of the phases is briefly described below.

Enrollment - Prior to an individual being identified or verified by a biometric device, the enrollment process must be completed. The objective of this enrollment process is to create a profile of the user. The process consists of the following two steps. The screenshots of the prototype are shown in figure also shown in figure 3:

1. Sample Capture: the user allows for a minimum of two or three biometric readings, for example: placing a finger in a fingerprint reader. The quality of the samples, together with the number of samples taken, will influence the level of accuracy at the time of validation. Not all samples are stored; the technology analyzes and measures various data points unique to each individual. The number of measured data points varies in accordance to the type of device.
2. Conversion and Encryption: the individual's measurements and data points are converted to a mathematical algorithm and encrypted. These algorithms are extremely complex and cannot be reversed engineered to obtain the original image. The algorithm may then be stored as a user's template in a number of places including servers and card.

A new and blank card has to be enrolled with user details before it can be verified later. Enrollment system is usually operated by the admin to enter their user's details into the card. However, the exception applies to the PIN entry where it should be entered by the user themselves and need to enter the PIN again to make sure they enter the correct ones.

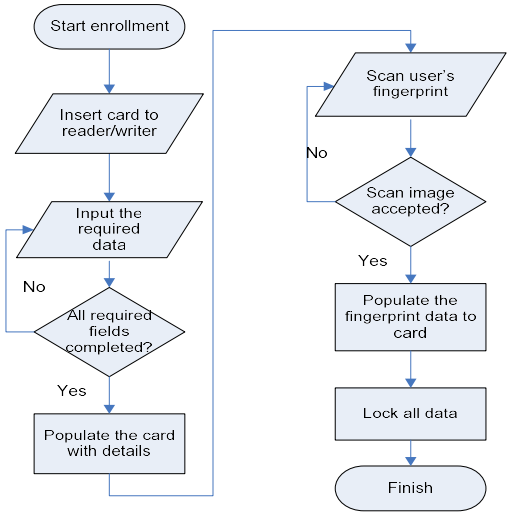

Figure2: Flowchart for the Enrollment Process

Figure3: Enrollment Process

Identification and Verification - *Once* the individual has been enrolled in a system, he/she can start to use biometric technology to have access the enrolled services from the fog database server. The screenshots of the prototype are shown in the figure also shown in figure 5:

1. Identification: a one-to-many match. The user provides a biometric sample and the system looks at all user templates in the database. If there is a match, the user is granted access, otherwise, it is declined.

2. Verification: a one-to-one match requiring the user provides identification such as a PIN and valid card in addition to the biometric sample. In other words, the user is establishing who he/she is and the system simply verifies if this is correct. The biometric sample with the provided identification is compared to the previously stored information in the database. If there is a match, access is provided, otherwise, it is declined.

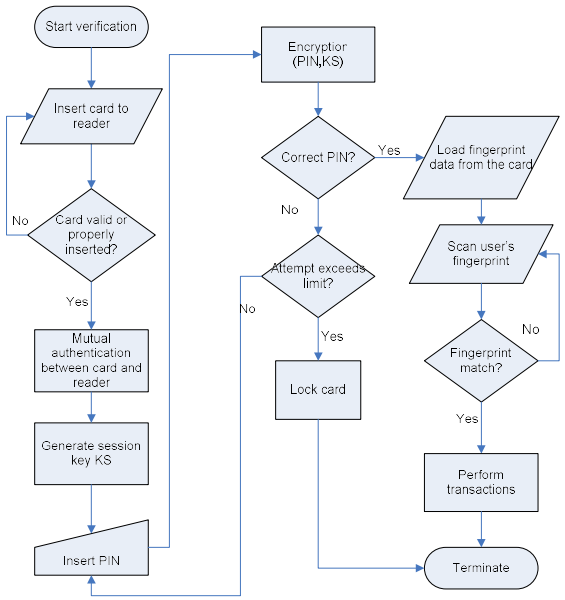

Figure4: Flowchart for the Verification Process

Figure5: Verification Process

After the card has been enrolled with user data, this particular card will be the user's ID. The PIN and fingerprint sample from the user wasalso encrypted and save into the card. In order to get access the fog server, the user has to present the card to the card reader, and then verify the PIN and lastly matched their fingerprint detail with the card. The sequence diagram in Figure 6 below summarizes the verification process.

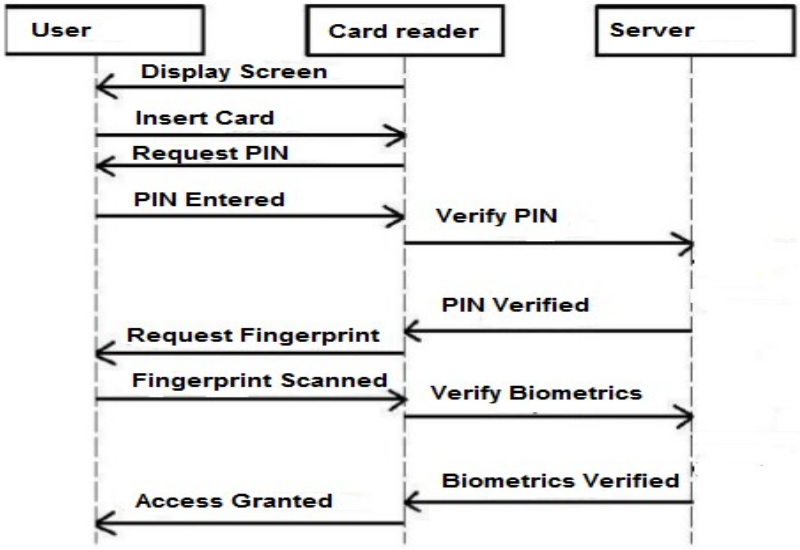

Figure 6: Process for granting access to service

5. CONCLUSION

In this paper, authors have explained the concepts of fog computing, and authors have presented the benefits, properties, and characteristics of fog computing and security issue related to it. On the other hand, authors have explained how to achieve the authentication of fog computing using the three-factor authentication method. Authors designed the new efficient model based on fingerprint, the implemented model works on storage all the user's fingerprints with their password on fog server

6. FUTURE STUDY

Biometrics increasingly form the basis of identification and recognition across many sensitive applications. But as the use of biometric systems increases, so do the threats against them. The secure storage of biometric templates has therefore, become a key issue in the modern era; the acceptance of biometric authentication devices by the general public is dependent on the perceived level of security of biometric information templates stored within databases. Privacy concerns have grown because a biometric template is a unique identifier of a person. And while the template cannot be decoded back to the biometric data, it may be used to track the individual. If there is a database that ties the user to their unique biometric template, it could be used illegally to monitor the activities of the user. Such threats need to be addressed, and one potential solution is cancellable biometrics. This is a template transformation technique that uses intentional repeated distortions to provide security to biometric templates; the distortions can be performed either at the signal level or at the feature level to achieve a transformed template. It is therefore important for further studies on cancellable biometrics and its application in IoT

REFERENCES

[1] Alrawais, A., Alhothaily, A., Hu, C., & Chang, X. (2017). Fog Computing for the Internet of Things: Security and Privacy Issues. IEEE Internet Computing, vol. 21, no. , pp. 34-42

[2] Balfanz, D., Smetters, D.K., Stewart, P., & Wong, H.C. (2002). Talking to strangers: authentication in ad-hoc wireless networks. Network and Distributed System Security Symposium (NDSS). San Diego, CA USA.

[3] Bonomi, F., Milito, R., Zhu, J., &Addepalli, S.(2012). Fog computing and its role in the internet of things. In Proceedings of the first edition of the MCC workshop on Mobile cloud computing. pp 13-16

[4] Maher, A.(2015). IoT, from Cloud to Fog Computing (Cisco Blogs). Retrieved November 02, 2018, fromhttps://blogs.cisco.com/perspectives/iot-from-cloud-to-fog-computing
Calandriello, G., Papadimitratos, P., Hubaux, J-P., &Lioy, A. (2007). , Efficient and robust pseudonymous authentication in VANET, in: Proc. VANET, pp. 19–28.

[5] Chang, C.,& Tsai, H.-C (2010). An anonymous and self-verified mobile authentication with authenticated key agreement for large-scale wireless networks, IEEE Trans. Wireless Communication. 9 (11) pp. 3346–3353.

[6] Cisco the network in review (2015). Retrieved September 02, 2017, from http://newsroom.cisco.com/featurecontent?type=webcontent&articleId=1365576

[7] Damiani, E., Vimercati, D.C., Paraboshi, S., Samarati, P., &Violante, F. (2002). A reputation-based approach for choosing reliable resources in peer-to-peer networks. Proc. of the 9th ACM conference on Computer and communications security, pp. 207-216.

[8] Deane, F.,Barrelle, K., Henderson, R., & Mahar, D. (2005). Perceived acceptability of biometric security systems. Computers & Security, Vol. 14, N. 3, pp. 225-231.

[9] Dsouza, C., Ahn, G.J., &Taguinod, M. (2014). Policy-driven security management for fog computing: preliminary framework and a case study". Proceedings of the 2014 IEEE 15th International Conference on Information Reuse and Integration (IEEE IRI).

[10] Gemalto (2018). Biometrics: authentication and identification (2018)- A case study. Retrieve 07 September, 2018, from https://www.gemalto.com/govt/inspired/biometrics

[11] He, D., Ma, M., Zhang, Y., Chen, C., & Bu, J. (2011). A strong user authentication scheme with smart cards for wireless communications, Computer Communications. 34 (3) 367–374.

[12] Josang, A., Ismail, R., & Boyd, C.(2007). A survey of trust and reputation systems for online service provision. Decis. Support Syst. 43(2), 618–644.

[13] Lu, R., Lin, X., Liang, X., & Shen, X. (2010). FLIP: An efficient privacy-preserving protocol for finding like-minded vehicles on the road, in: Proc. IEEE Globecom, pp. 1–5.

[14] Luca, B., Bistarelli, S. &Vaccarelli, A. (2002). Biometrics authentication with smartcard. IIT TR-08/2002, Retrieved October, 9, 2017, fromhttp://www.iat.cnr.it/attivita/progetti/parametri biomedici.html

[15] Modi, C., Patel, D., Patel, H., Borisaniya, B., Patel, A. & Rajarajan, M. (2013). A survey of intrusion detection techniques in Cloud. Journal of Network and Computer Applications, 36(1), pp. 42-57

[16] Renu Bhatia (2013), Biometrics and Face Recognition Techniques, International Journal of Advanced Research in Computer Science and Software Engineering Vol. 3, Issue 5, pp 93-99

[17] Sean W. S. & Vernon A. (1998). Trusting Trusted Hardware: Towards a Formal Model for Programmable Secure Coprocessors. Proceedings of the 3rd USENIX Workshop on Electronic Commerce. Boston, Massachusetts, USA.

[18] Shanhe, Yi,.Zhengrui, Q., &Qun, Li. (2015). Security and Privacy Issues of Fog Computing: A Survey. Proc. Int'l Conf. Wireless Algorithms Systems and Applications (WASA) 2015, LNCS 9204, pp. 685–695.

[19] Shi, Y., Abhilash, S., & Hwang, K.(2015). Cloudlet mesh for securing mobile fogs from intrusions and network attacks. In: 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering. pp. 1096-118

[20] Stojmenovic, I., & Wen, S.(2014). The fog computing paradigm: scenarios and security issues. In: Proc. of the 2014 Federated Conference on Computer Science and Information Systems (FedCSIS) conference. pp. 1-8.

[21] Tsai, H., Chang, C., & Chan, K. (2009). Roaming across wireless local area networks using SIM-based authentication protocol, Computer Standard Interfaces 31 (2) pp.381–389.

[22] Tsai, Y. & Chang, C. (2006) , SIM-based subscriber authentication mechanism for wireless local area networks, Computer Communications. 29 (10) pp. 1744–1753.

[23] Vaquero, L.M., &Rodero-Merino, L. (2014). Finding your way in the fog: towards a comprehensive definition of fog computing. ACM SIGCOMM CCR44(5), 27–32

[24] Zhu, H., Lin, X., Lu, R., Ho, P., & Shen, X. (2008). AEMA: An aggregated emergency message authentication scheme for enhancing the security of vehicular Ad Hoc networks, in: Proc. IEEE ICC, pp. 1436–1440.

[25] Calandriello, G., Papadimitratos, P., Hubaux, J-P., &Lioy, A. (2007). , Efficient and robust pseudonymous authentication in VANET, in: Proc. VANET, pp. 19–28.

[26] How to Geek (2014). What is Fog Computing? Retrieved September 02, 2017, From https://www.howtogeek.com/185876/what-is-fog-computing/

Author

Kashif Munir received his BSc degree in Mathematics and Physics from Islamia University Bahawalpur, Pakistan in 1999. He received his MSc degree in Information Technology from University Sains Malaysia in 2001. He also obtained another MS degree in Software Engineering from University of Malaya, Malaysia in 2005. He completed his PhD in Informatics from Malaysia University of Science and Technology, Malaysia. His research interests are in the areas of Cloud Computing Security, Software Engineering, and Project Management. He has published journal, conference papers and book chapters.

Kashif Munir has been in the field of higher education since 2002. After an initial teaching experience with courses in Stamford College, Malaysia for around four years, he later relocated to Saudi Arabia. He worked with King Fahd University of Petroleum and Minerals, KSA from September 2006 till December 2014. He moved into University of Hafr Al-Batin, KSA in January 2015.

Kashif Munir is a researcher and published author/editor of 4 books on cloud computing including subjects such as Security in Cloud Computing, Mobile Cloud and Green Enterprises, (https://www.amazon.com/Kashif-Munir/e/B079KP1LFJ).

Lawan A. Mohammad, Holds a PhD degree in computer and communication systems engineering from University Putra Malaysia. Research interest include smartcard security, authentication protocols, wireless and mobile security, biometrics, mathematical programming and e-learning.