IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 30, 2017, accepted December 1, 2017, date of publication January 3, 2018, date of current version March 9, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2789301

Vulnerability Analysis for the Authentication Protocols in Trusted Computing Platforms and a Proposed Enhancement of the OffPAD Protocol

MADA ALHAIDARY[1,3], SK MD MIZANUR RAHMAN[1,3], MOHAMMED ZAKARIAH[4], M. SHAMIM HOSSAIN[2,3], ATIF ALAMRI[2,3], MD SARWAR M HAQUE[5], AND B. B. GUPTA[6]

[1]Department of Information Systems, College of Computer and Information Sciences, King Saud University, Riyadh 11451, Saudi Arabia
[2]Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11451, Saudi Arabia
[3]Chair of Pervasive and Mobile Computing, College of Computer and Information Sciences, King Saud University, Riyadh 11451, Saudi Arabia
[4]College of Computer and Information Sciences, King Saud University, Riyadh 11451, Saudi Arabia
[5]Department of Computer Science, King Fahd University of Petroleum & Minerals, Dammam 34463, Saudi Arabia
[6]National Institute of Technology Kurukshetra, Kurukshetra 136119, India

Corresponding author: M. Shamim Hossain (mshossain@ksu.edu.sa)

This work was supported by the Deanship of Scientific Research, King Saud University through the Vice Deanship of Scientific Research Chairs.

ABSTRACT Trusted computing architecture ensures the behavior of software that runs on a user machine by protecting software-level attacks. Due to the potential of exposing a user's private information while accessing a system, many studies have focused on analyzing existing protocols to develop new methods based on biometrics or additional devices to add new layers of security to the authentication process. For a few years, the idea of utilizing the combination of *something you know* with *something you have* and a *personal authentication device* (PAD) has become common in verification protocols. Very recently, a more secure PAD, namely the Offline Personal Authentication Device (OffPAD), was invented to improve the authentication process. This single device can be used to manage the identities of both users and service providers as well as support the authentication process, while being offline most of the time. In this paper, a rigorous vulnerability analysis for OffPAD-based authentication techniques is conducted using an attack tree analysis. Finally, to overcome the vulnerabilities, mitigation techniques are proposed.

INDEX TERMS Data origin authentication, entity authentication, biometric authentication, offline personal authentication device (OffPAD), vulnerability analysis.

I. INTRODUCTION

Trusted computing (TC) refers to a cluster of ideas, technologies and applications for resolving computer security problems. It ensures that different parts of the system are behaving as expected. This improves the overall trustworthiness, privacy and security of hardware and software [36] and allows applications to communicate securely with servers and other applications. TC can be achieved through software modifications and hardware enhancements. In PC hardware, encryption keys are built that can be used to verify its identity and integrity. The operating system guarantees the application software's character and integrity by communicating with remote servers securely. To achieve secure operations, hardware-based cryptographic keys are used, which are generated and stored in the hardware manufacturing process. The design of this hardware is so sophisticated that it is not possible to retrieve the key by any method (i.e. reverse engineering). This core is never exposed to any other component – even to the owner. Many applications use the concept of TC, for example, digital rights management, different platform authentication, preventing cheating in multiplayer games, distributed firewalls, third-party computing, improving reputation reckoning and data security and privacy [40].

Authentication is an essential security service and a critical method for determining whether an individual is who s/he claims to be. It is usually based on a username and password, with supporting hardware, which can improve a service's security. Therefore, authentication is considered to be a significant issue for online service access. As authentication is necessary for individuals to guarantee that their accounts are secure and their information is not exposed to everyone, it is also essential for organizations to have an

authentication method in their information systems. In general, there are many reasons why organizations should implement user authentication besides security reasons, including monitoring system activities, filtering incoming and outgoing content to configure role sets and policies and managing time allowances by specifying the total duration of system access for each user.

Acknowledged authentication factors have been placed into three categories, each of which may contain a range of elements used to verify and authenticate the identity of an individual. The classes are as follows: first, *knowledge factors* (what a user knows), for example, the password; second, *ownership factors* (what the user has), for example, an ID card; and third, *inherent factors* (who the user is), such as fingerprint data. A more useful approach is to combine two or more authenticator factors to gain benefits in security, convenience or both; for example, an ATM requires a bank card and a PIN. The bankcard is an example of something a user has and the PIN is an example of something a user knows. In this case, to represent this scenario, the preferred term is two-factor authentication [3]–[7].

Because of the vulnerability of standard passwords, it is critical to manage them appropriately and it is essential to have a high level of certainty when identifying and authenticating users. Further control efforts are needed, but, with large systems, this may prove difficult. Fortunately, there is a more straightforward solution for adding a second layer of security to user logins and transactions that can be granted using multi-factor authentication. This solution works by involving two or more different factor criteria [8]–[10].

Online service access usually uses a combination of static passwords and hardware devices, which dynamically generate access credentials. This approach requires that the user has many tools for each transaction and more passwords than s/he can memorize. To manage this situation, the personal authentication device (PAD) was proposed; the PAD can be used for user authentication for every online service, in addition to providing a series of other security services. By using the PAD as an identity manager, the user can be authenticated by every supported service automatically. The authentication process can be achieved by passing replay-protected challenge-response communication between the PAD and remote servers [11]–[15].

Varmedal *et al.* [1] proposed an advanced PAD, called the Offline Personal Authentication Device (OffPAD), which provides authentication and identity management for both user and service provider. The main advantage of the OffPAD is that it is more secure than a standard PAD; by being offline most of the time and including safe components, OffPAD can defend its content and user privacy.

In this paper, the mitigation techniques for protecting the vulnerabilities of OffPAD-based authentication solution has been proposed, which is the extended version of their previous work [37]. The limitation of the proposed technique is that it is not studied the implementation of the solution in a hostile environment.

A. REVIEW OF THE OffPAD

Using two-factor authentication is an authentication category that combines *something a user knows* with *something a user has*, as with a bank account security token. A more advanced device that can be used for multiple systems at the same time is the PAD, which can provide security, privacy and multi-service authentication using just one device.

Varmedal *et al.* [1] also proposed a new, more secure version of the PAD, called the OffPAD. This new version supports the management and authentication of both service provider and user identities. The primary goal of this device is to provide the user with tools for securely managing the authentication processes for online transactions, by avoiding man-in-the-middle and phishing attacks while managing online identifications. Franks *et al.* [2] first published details of the PAD in 2005. Then, in 2013, the OffPAD was proposed by Varmedal *et al.*

The authentication process can be achieved by passing replay-protected challenge-response messages among the PAD and isolated servers; the OffPAD never exposes the password to the client terminal and remains online for brief periods only. Thus, the devices are minimally exposed to the distant server through the operator's computer. Therefore, the OffPAD can be used as:

1. A password/identity management system, controlling the end user's identifications for several services.
2. A service authenticator that can be used by a company, by which the user is validated once for each session, whether by PIN or similar.
3. A transaction signature, used by the user to sign data electronically. By using the PAD as a user identity manager, authentication can be achieved automatically by every supported service.

B. USING AN OffPAD TO MANAGE AND AUTHENTICATE A USER

Usually, a password is either entered by a user or decrypted by a password manager to access systems, but in this traditional scenario, the password is vulnerable to attacks; it is exposed to the computer memory, which means threats to authentication. By contrast, the OffPAD uses the HTTP Digest Access Authentication (DAA) system identified as a portion of the HTTP standard in [3]. It uses a hash function to store the user's identifications on both the server and the OffPAD. The authentication scenario is as follows:

- **a.** The session starts with the client sending a request for a sheltered resource.
- **b.** The server sends the response with an verification test.
- **c.** The authentication challenge is muddled with the client identification and sent to the server by the client.
- **d.** The similar test response counts are done locally by the server, which afterward associates the outcome with the response. Once the examination is

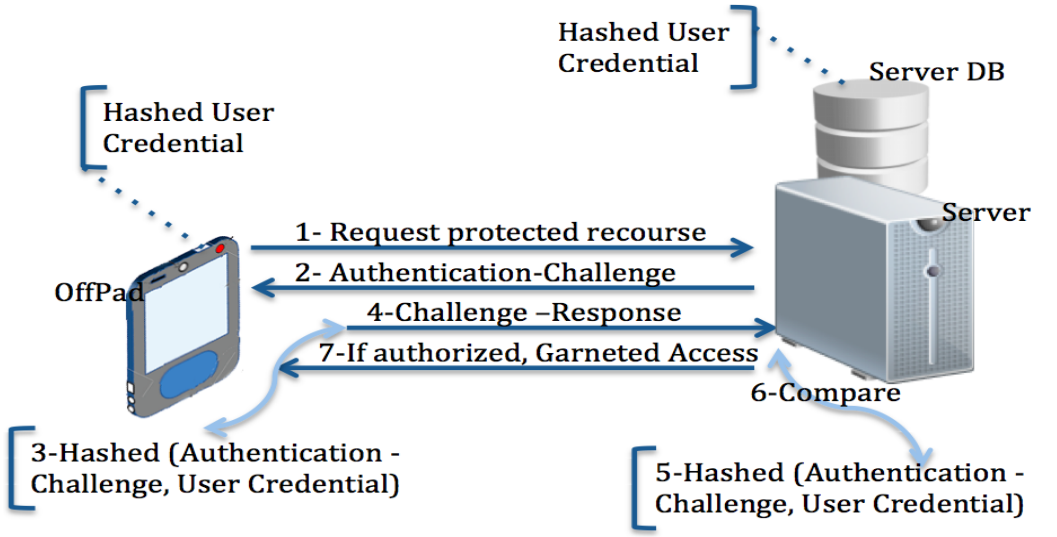

FIGURE 1. OffPAD authentication scenario.

completed successfully, the client is allowed access to the asset. This situation is shown in Figure 1.

II. LITERATURE REVIEW OF RELEVANT RESEARCH

By exploiting the unrevealed vulnerabilities in existing authentication protocols, an attacker can gain a considerable amount of illegal benefits. Therefore, many studies have focused on the analysis of existing protocols to develop new methods that add more layers of security, either based on biometrics or using extra devices. Based on this, we conducted a rigorous literature review on the existing protocols with a detailed classification and the taxonomy is provided in Fig. 2.

A. CLASSIFICATION BASED ON AUTHENTICATION ANALYSIS

1) ANALYSIS OF WIRELESS AUTHENTICATION

Antonysamy and Patro [4] highlighted the ''challenges and possibilities of antenna design for the multipurpose wireless authentication device,'' which includes the interface, control of the internal devices, product certification issues and interference with other wireless technologies.

2) AUTHENTICATION SETS TO ANALYZE SECURITY ISSUES

To examine the security of a *secure multimedia authentication scheme*, [5] proposed a new technique, called an *authentication set*. A definition of many of the original concepts of authentication was proposed, such as *cover "authentication sets*, *attack authentication sets*, *watermark-based authentication set*s (or *signature-based authentication sets*), *verified authentication sets"* and ''*malicious-attack authentication set*s''.

3) ANALYSIS OF VERIFICATION SYSTEMS FOR WIRELESS SENSOR NETWORKS [6]

Seven operator verification systems for wireless sensor networks against 22 features were evaluated by [7]. They aimed to introduce the importance of developing new verification systems that take into account all the elements discussed, which can then provide a set of guidelines for future schemes proposed in the research. From their evaluation, they realized many things: first, the failure of all existing schemes to protect against gateway node bypassing attacks, node capture attacks and user impersonation attacks; second, that mutual authentication that resists denial-of-service attacks is provided by only one scheme.

4) ANALYSIS OF THE PAIRHAND PROTOCOL

Reference [8] analyzed a recently proposed handover authentication protocol, PairHand, to discover its vulnerability. They identified a threat to a compromised session key and tried to compromise it through a simple modification of the protocol, without losing any features. PairHand is very efficient in terms of computational complexity and communication, because of its features of shared verification and essential formation; only two handshakes are needed in between MN and AP, with no requirement to transmit any verification certificate as is done in traditional public key cryptosystems [9].

5) ANALYSIS OF Li-Hwang's PROTOCOL

Reference [10] investigated Li-Hwang's biometrics-based distant operator verification system by utilizing smart cards and discovered some configuration defects. In the login and confirmation stages, they found that the framework superfluously includes additional correspondence and calculation. Second, during the password change phase, there was no verification of the old password in the scheme, even if the user entered his old password incorrectly by mistake; updating the new password would take place mistakenly. Finally, they discovered a flaw in the biometric checking hash; when the biometrics information was noisy, the cryptographic hash

capacity could not be clearly connected. With the specific goal of overcoming these defects, he proposed changes to the plan.

6) ANALYSIS OF THE CPN (COLORED PETRI NET) PROTOCOL

To protect trusted platform module objects from unauthorized access, some alternatives have used an object-specific authorization protocol (OSAP) or session key authorization protocol (SKAP). By using this situation as a case study, [11] examined the security analysis value of CPNs to demonstrate their applicability as a common device for modeling and analyzing safety procedures. By including error handling and the recovery of many parts of the model, error discovery was improved. This proposed method is done by examining the OSAP to enhance the SKAP.

7) ANALYSIS OF THE AKA PROTOCOL

The first computational security analysis of both the LTE AKA and the UMTS AKA was by [12]. They found a vulnerability that both inside and outside attackers could exploit. An inside attacker might be authenticated as another owner subscribed to a helping network and use wireless facilities on the owner's behalf, while an outside attacker might defeat the entity authentication of the user to the serving networks. They also investigated the vulnerabilities of the stipulations of the UMTS and LTE AKA (and GSM IA) protocols [12]. Since they all use the 3rd Generation Partnership Project, both outside and inside attackers could take advantage of this flaw, by using the computationally proven CryptoVerif to violate the entity authentication properties.

8) ANALYSIS OF A "MORE EFFICIENT AND SECURE DYNAMIC ID-BASED REMOTE USER AUTHENTICATION SCHEME"

The authors of a "more efficient and secure dynamic ID-based remote user authentication scheme" declared that their scheme preserves client secrecy, but [13] suggested that it does not. During authentication, the user cannot choose his/her password, which makes him/her vulnerable to insider attacks. Hence, the scheme is not feasible for real-life implementation.

9) ANALYSIS OF FACEBOOK CONNECT

The method in [14] warned of attacks on the authentication protocol of Facebook Connect, detected by analyzing the HLPSL formalization presented when using the Automated Validation of Internet Security Protocols and Applications (AVISPA). Facebook platforms offer a single sign-in service that allows users to log in to affiliated sites. The authors exposed two security weaknesses; correctly, that the Facebook Connect verification procedure is adhered to repetition attacks and masquerade attacks.

10) ADDRESSING THE VULNERABILITIES OF LOGIN CREDENTIALS BY ANALYZING CHARACTERISTICS

Reference [15] tried to address the vulnerabilities of login credentials by analyzing the characteristics of login credential usage and found that the number of subscriber accounts was considerably more significant than previously expected. They also found that many users used the same login credential information as each other.

11) ANALYSIS OF RFID

Li and Deng [16] proposed a mutual authentication protocol for RFID. Li and Deng (2007) analyzed the security vulnerabilities of this new protocol and found two potential attacks against it: a DE synchronization attack and a full disclosure attack. This work [17] was based on tripartite credibility to present a secure mechanism and enhance the security of LLRP and a third-party authentication system. It has two steps: first to describe the relevant information about the design of RFID and then to evaluate its performance based on storing difficulty, expense on communication and computational cost as well as to analyze the safety rewards compared with those of earlier research.

12) ANALYSIS OF TRMA+

To enhance the Class-1 and Generation-2 standard of RFID which is described in [18], Peris-Lopez *et al.* proposed a new version of the TRMA scheme (TRMA+). However, they showed that this new version still contains severe security defects [19]. It is easy to recover 32-bit access and destroy passwords for a tag under the TRMA+ scheme by the attacker [20].

B. ONE-FACTOR PROTOCOLS

1) MULTI-LEVEL PASSWORD GENERATION

In this work, Dinesha and Agrawal [21] suggested a method of accessing a cloud service that involves generating the password at many levels across the organization, which provides strict authentication and authorization. Their technique contains two separate objects: first, to ensure the cloud services, they have a cloud service provider; and second, they have an authenticated client organization for those accessing the cloud service. Authentication activities can be applied at the agency, team and user levels.

2) STAGGERED TESLA

Li and Trappe [22] established *staggered timed efficient stream loss-tolerant authentication* (TESLA) as new a multi-grade multicast authentication scheme used when creating the MACs for authenticating a packet, by employing staggered and multiple authentication keys. Their method is useful to compromise the effects of DoS attacks by using multi-grade authentication in multicast scenarios and enhances the filter forged multicast packets by reducing the delay.

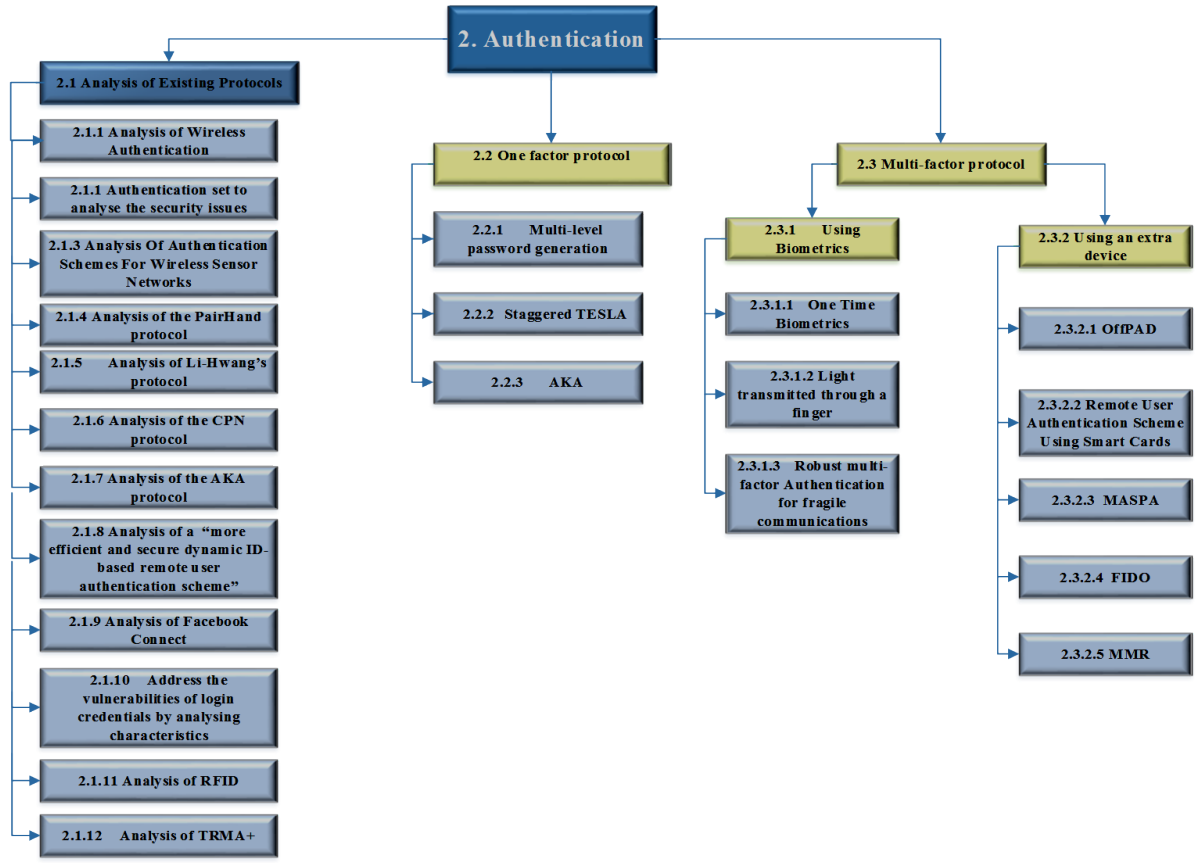

FIGURE 2. Taxonomy of the protocols.

3) AKA

Huang and Li [3] proposed a one-pass authentication and key agreement (AKA) protocol that avoids the existing efficiency problem. In this work [23], a smart car-based user AKA security protocol is developed for the Telecare Medical Information System with the help of a cryptographic one-way hash function and the results are simulated by using the AVISPA tool. The outcome of the experiment is secure against replay and man-in-the-middle attacks.

C. MULTI-FACTOR PROTOCOLS

1) USING BIOMETRICS

In the following subsections, the multifactor biometric-based protocols are described.

a: ONE-TIME BIOMETRICS

Plateaux *et al.* [24] proposed a new authentication protocol for online banking and electronic payment systems called *one-time biometrics*. Their protocol involves two main components: the OffPAD, which ensures security and privacy, and a supporting biometrics algorithm. The protocol demonstrates outstanding performance when applied to three levels of fingerprint databases, and has great properties for safety and protection issues. A challenge-based procedure is then planned to stop replay attacks. The study focused on making online banking transaction authentication more robust by analyzing how to use biometrics with user authentication.

b: OPTICAL DEVICE FOR FINGERPRINT AUTHENTICATION

Sano *et al.* [25] proposed a device that supports a new fingerprint algorithm. This new device considers the optical characteristics of the finger to form an image of the fingerprint pattern. The user's prints provide secure authentication and are not affected by changes in the state of the finger or operating environment. The device can also sense false fingerprints that are made from jelly or other materials.

c: ROBUST MULTI-FACTOR AUTHENTICATION FOR FRAGILE COMMUNICATIONS

Reference [26] proposed two solutions for verification in unstable communication surroundings. The first solution is a protocol based on using passwords, smart cards and biometrics, which provides a promising verification explanation in slow-connection circumstances called multi-factor authentication protocols. The second solution is stand-alone authentication, which allows users to be adequately authenticated regardless of the status of their connection to the remote authentication server.

2) USING AN EXTRA DEVICE

a: OffPAD

The OffPAD aims to provide the user with tools for securely managing the authentication processes for online transactions, by avoiding man-in-the-middle and phishing attacks and managing online identifications at the same time. Jøsang and Pope first published details of the PAD in 2005 [2]. Then, in 2013, [1] proposed an improved version of the PAD: the OffPAD. To protect user privacy and device contents, it is intended to remain offline most of the time and contains a secure element.

b: REMOTE USER AUTHENTICATION SCHEME USING SMART CARDS

Another study [27] suggested using a smart card to support operator verification, grounded on ElGamal's public key cryptosystem. The card's security trusts on the effort of calculating discrete logarithms above finite fields. This is a system of remote user authentication without a password verification table; the user applies to the registration center and is issued with a smart card with a password. After this, when the authorized user wants to log in, s/he inserts the card into the login device along with his/her ID and password.

c: MASPA

Reference [28] discussed a mobile architecture for strong personal authentication (MASPA), which uses hash functions, symmetric and asymmetric encryption (a three-pass Diffie-Hellman variant) and cryptographic primitives including digital signatures in its authentication algorithm.

d: FIDO

Reference [29] attempted to provide an authentication mechanism (FIDO) that reduces reliance on passwords. The new verification structure intends to give a favorable split between local-user-to-authenticator authentication and authenticator-to-reliant-party authentication; trusted parties can utilize the new client verification strategies without changing the server-side infrastructure.

e: MMR

Although mobile multi-hop relay (MMR) is a self-organizing and self-healing network, due to its nature, it is vulnerable to security threats. In [30], a centralized authentication and key distribution algorithm were discussed for MMR.

III. VULNERABILITY ANALYSIS FOR AUTHENTICATING A USER BY USING THE OffPAD

A. POSSIBLE VULNERABILITIES OF SINGLE- AND MULTI-FACTOR AUTHENTICATION PROTOCOLS

This section outlines some of the ways in which protocols may fail to meet their goals. The partial investigation of vulnerabilities, concerning an attack tree of existing single- and multi-factor authentication protocols such as AKA, MMR and TESLA [12], [19], [22], [31], [32] is illustrated in Figure 3.

Ming *et al.* investigated AKA and found that it was vulnerable to man-in-the-middle, session hijacking and server spoofing attacks, among others [12]. Additionally, it found vulnerability that both inside and outside attackers could exploit. TESLA aims to have an efficient protocol to minimize the communication and computation overheads, but it is still vulnerable to DoS attacks and delayed packets.

B. THREATS AND ATTACKS WHEN USING THE HTTP DAA PROTOCOL WITH THE OffPAD

As previously discussed, Klevjer *et al.* proposed an improvement to password authentication with the OffPAD, which uses an HTTP DAA scheme identified as a part of the HTTP standard [3]. DAA is a web server method that can be used to verify both parties to a communication. The main idea behind DAA is to apply a cryptographic hash on the user credentials to produce the message digest, which is then sent over the communication network. One example is online banking transactions.

DAA was first announced by RFC 2069, which is an Extension to HTTP: DAA. DAA uses a server generated nonce to add security to the traditional digest authentication scheme. Optional security improvements to DAA were introduced, replacing RFC 2069 with RFC 2617 (HTTP Authentication: Basic and DAA) [33].

The security choices in RFC 2617 are discretionary; if the server does not specify the security options, then the user may work in the less-secure RF 2069 mode. In this section, we discuss the attacks that can be caused by using the HTTP DAA protocol to authenticate users aligned with the OffPAD. We discovered two attacks.

1) MAN-IN-THE-MIDDLE ATTACKS

Using DAA made the authentication process vulnerable to man-in-the-middle attacks. While DAA does not provide any mechanism to verify the server's identity for clients, the intruder can fool the client by impersonating the server and asking to use the legacy RFC 2069 DAA mode that does not support the optional security enhancements.

A man-in-the-middle attack could occur when a weak authentication scheme is added to the user options by the intruder, which may reveal the client's identifications. Therefore, the client should be aware and always select the most reliable scheme from the selections offered [2].

2) REPLAY ATTACKS

The DAA security option enhances basic authentication and makes it safer against eavesdropping attacks, but it is still vulnerable to replay attacks.

If the server only supports the nonce, the intruder can eavesdrop on a message or message components from a previous session and replay it as a new message to establish a new course [34]. Even the user credentials are hashed and sent to the server as a digest. The intruder can use this compendium without knowing the password by capturing it and replaying it to the server to establish a new session.

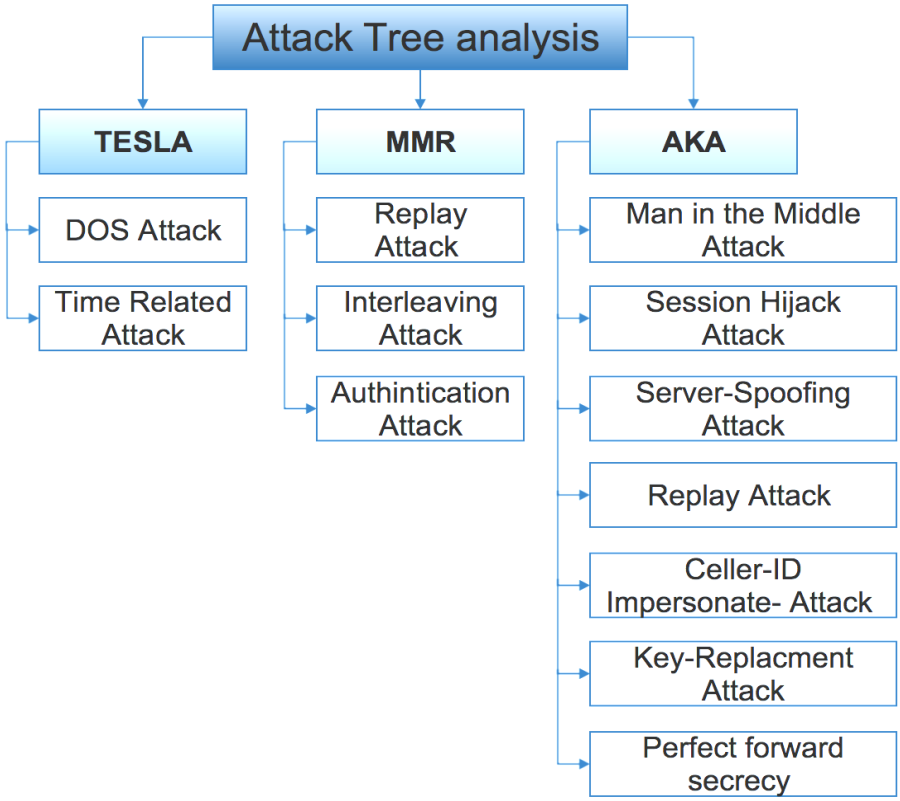

FIGURE 3. High-level attack tree analysis.

IV. PROPOSED SOLUTION

This section discusses a mitigation technique for man-in-the-middle and replay attacks and then suggests principles to guide the design of further secure authentication schemes. The complete procedure is displayed in the Figure 4 and the details are listed in the steps below:

1. The client and server contact a third-party certificate authority to sign a certificate that binds *identity* to a *public key*.
2. When secret recourse is requested, the client and server exchange their certificates to verify each other's identity. At this point, the verification phase ends. This helps maintain the session against a man-in-the-middle attack.
3. The server then sends a Challenge, which contains an authentication challenge along with a nonce and time stamp.
4. The client computes the session key K_S = Hash (authentication Challenge || nonce || time stamp), and then sends it back to the server as a response. This is the reply of the challenge of the server from the client side and the part of the challenge-response mutual authentication.
5. The server computes the session key K_S and compares it with the one received from the client. This is the verification of the response at the server side.
6. If the computation is equal, then access is granted; thus the challenge-response authentication successes.

As a conclusion, we present some proposed solutions to mitigate each attack.

A. MAN-IN-THE-MIDDLE ATTACKS

This attack can occur by adding a weak authentication scheme such as the RFC 2069 DAA mode that does not support the optional security enhancements to the set of options, expecting that the user will select this scheme, which can expose his or her cardinal.

For this reason, we suggest possible solutions against this attack. First, the client should be aware and always select the most reliable scheme that s/he knows from the selections presented. Second, for high-risk and high-security systems that require these guarantees, the user has to turn to Secure Socket Layout (SSL). SSL is a transporting layer security, where the client and server exchange PKI certificates before establishing a session; these certificates are issued and verified by a third party, which should be a standard certificate authority [2].

B. REPLAY ATTACKS

To prevent replay attacks, the server can pass a dynamic token called a server-specified nonce to the client, which is changed frequently [33]. The client attaches this nonce token to the

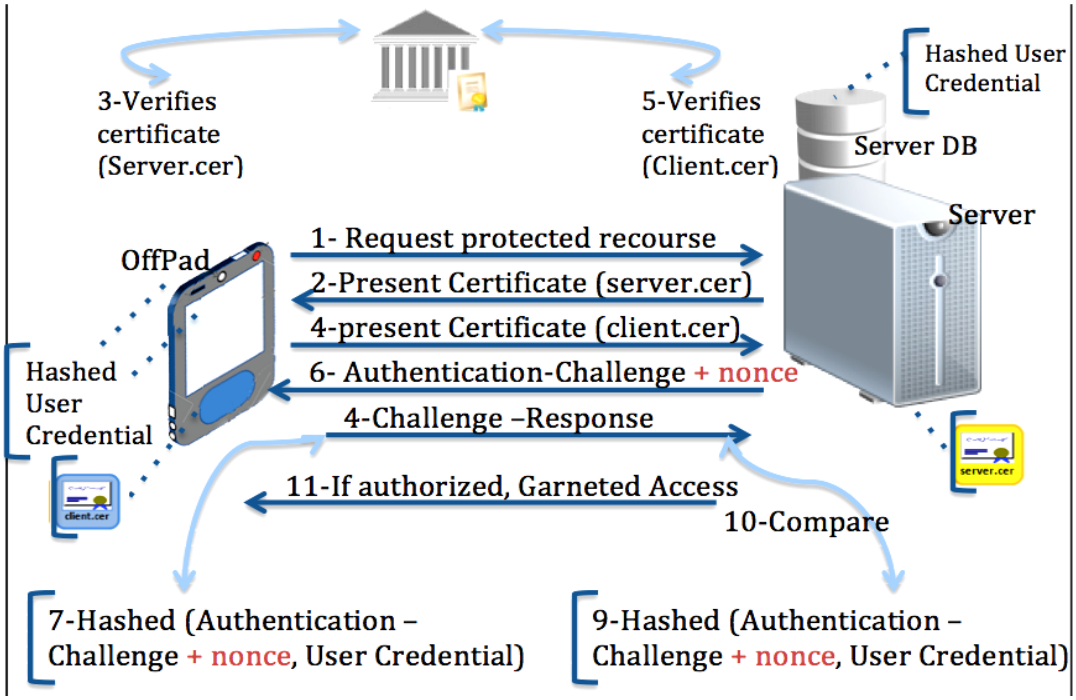

FIGURE 4. Illustration of the proposed enhancement to the OffPAD authentication protocol.

password before computing the digest and it can be used as a password salting. Mixing the nonce in the password by concatenating it causes the summary to change each time the nonce changes. Thus, the replay attack is prevented [35].

C. COMMUNICATION AND COMPUTATIONAL COST

The protocol has five interactive handshake communications between the sender and the receiver for mutual authentication with the standard certificate and TCP/IP packets. On top that the protocol needs to compute, two concatenation operations and two hash functions computation.

V. IMPLEMENTATION AND SECURITY ANALYSIS

In this section, first, the implementation using a security tool for the formal verification of the proposed protocol is discussed. In the next subsection, an analysis is provided.

A. AVISPA: A VERIFICATION TOOL FOR FORMAL SECURITY ANALYSIS

AVISPA is considered to be one among the most reliable, programmed official secured, verified and analysis tools for secure communication protocols. It has the capability of verifying whether or not the security protocol is secure and is capable of displaying every possible attack and its traces in case it is not entirely secured. AVISPA, which is freely available, makes it easy to model any security protocol. It has an animated and instinctive language known as High-Level Protocol Specification Language (HLPSL) to help the procedure writer and check the specification of the protocol. The basic idea about HLPSL has been derived from the semantic roots of Lamport's Temporal Logic of Actions [38]. It also permits complex stream of designs and data structures and gets them exposed. Aslo, it displays the communication method happening between different agents with the help of the "Alice-Bob" notation. The language used to define the protocol is based on various roles and each role is played by an agent. Depending on the position assigned, each agent has to perform its task. The primary job assigned for the purpose is usually an event action-dependent transition: the moment an event happens; the agent has to act accordingly by moving itself from one state to another after the completion of a particular action. Furthermore, there is always a relation between an event or an action from any agent and an occasion or act from any of the lasting mediators; to be clear, when something is sent or received by the agent, there is continuously extra mediators who acts on it either as receiver or as sender depending on the action happened.

Additional kind of character is also available called the composed role. This role acts as an initiator; it helps modelling the whole protocol and generates a session with multiple agents. When this role executes the complete procedure, then it is named as the chief role or the atmosphere role. Once this role is described, there is a need to set the security goals in HLPSL. AVISPA is used to execute the protocol defined and modeled by HLPSL to verify its back-end to check its security goals. The well-known intruder model in [39] is used by AVISPA, which expects an intruder to interfere inside the network and take command of network traffic as much as possible, which helps in making the analysis. Moreover, it also helps define the knowledge of the intruder in the HLPSL model.

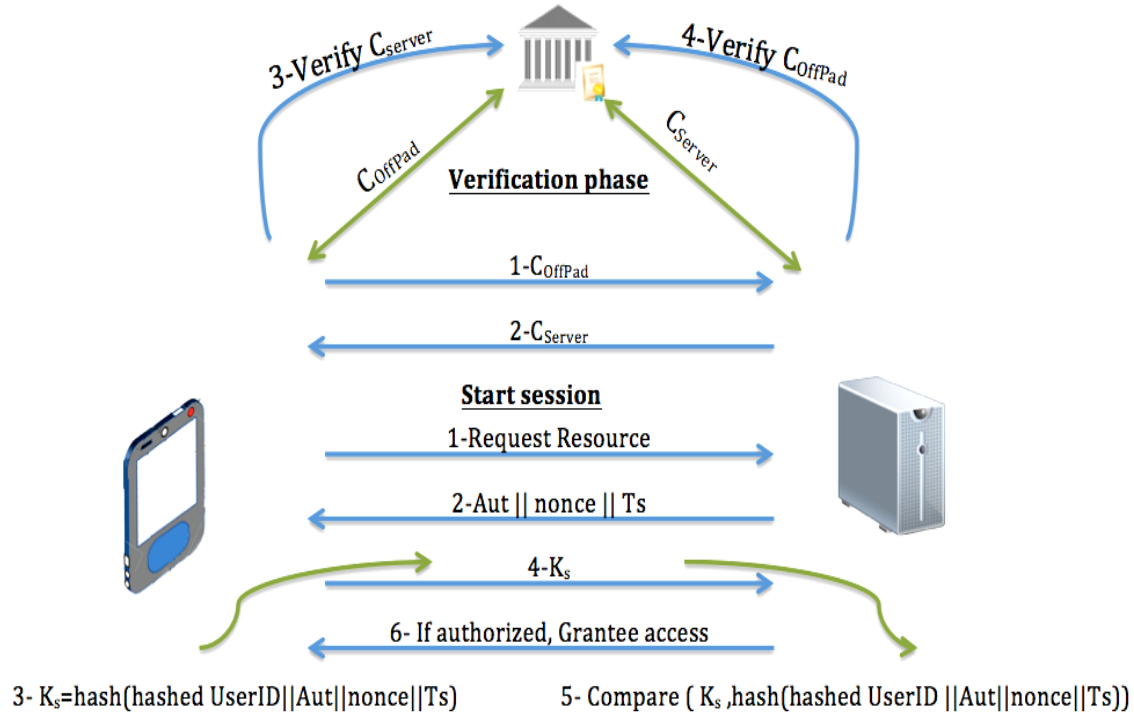

FIGURE 5. Illustration of the proposed enhancement to the OffPAD authentication protocol.

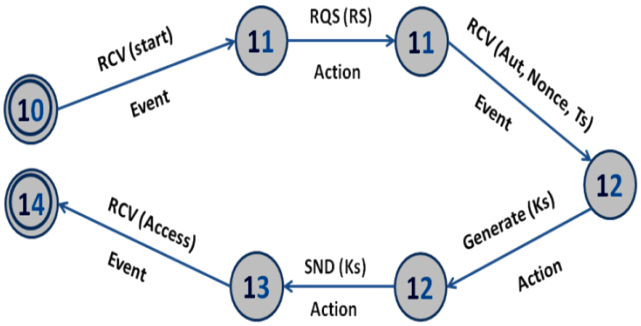

FIGURE 6. State transaction for the PffPAD.

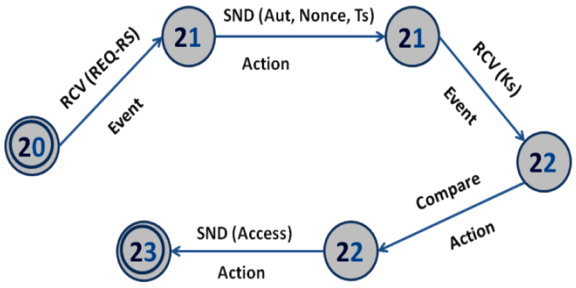

FIGURE 7. State transition for the server.

B. SECURITY ANALYSIS

In this section, the formal verification of security analyses for the proposed solution is discussed. As mentioned previously, we use AVISPA for simulation and formal verification. To this end, the HLPSL and CAS+ models of our proposed solutions are presented, as they are an easy way in which to model a protocol characterized in the Alice-Bob notation, since this gives a perfect vision of the communication among the parties. The first proposed solution is represented in the Alice-Bob notation, as illustrated in Figure 5. From the figure the steps are easily understandable, only step 3 and 5 need to discuss little-bit for better clarification. In step 3 the key has been computed and in step 5, the received and computed values has been compared.

The HLPSL Model For The Proposed Protocol: Using the Alice-Bob notation in Figure 5, the automata format representation is depicted in Figures 6 and 7, where the state transitions are shown openly for all the essential roles (OffPAD, server). HLPSL works in the event action-based model, which is why ''event'' and ''action'' are attached with the transitions. Due to the scope limitations of the paper, a few important things are discussed here regarding the HLPSL model for the proposed protocol. The keyword ''RCV'' is used to receive a message from a sender and ''SND'' is used to send a message to a receiver. HLPSL has a default ''start'' state for the initiator to start the protocol. In our model, the OffPAD takes the initiative for the initial communication by sending a special signal ''SND(start).'' In HLPSL, it is assumed that the roles have some pre-computed shared knowledge to start the protocol. Based on this pre-computed shared understanding between the roles, the proposed protocol is executed in the HLPSL model. It is remarked by the AVISPA state transition that both of the roles are in a safe state. An intruder party cannot have enough knowledge to attack the protocol.

VI. CONCLUSION

The target of this paper was to investigate the possible vulnerabilities of OffPAD-based solutions and provide mitigation techniques for these vulnerabilities. Many studies focus on the analysis of the potential to expose a user's privacy while accessing a system through an authentication process. By conducting a detailed classification and rigorous literature review on existing protocols, we showed the existence of different protocols that use extra devices or biometrics. Subsequently, we performed a partial investigation of the vulnerabilities in some actual data origin and entity authentication protocols, using an attack tree analysis. We realized that there are many forms of attacks that could threaten the privacy of the user through these protocols. concerning the previous sections, a vulnerability analysis for OffPAD-based solutions for user authentication was performed. As a consequence of our security analysis, we found that this authentication was vulnerable to attacks, specifically replay and man-in-the-middle attacks; therefore, to mitigate these attacks, new schemes were presented by using SSL and nonces to prevent them. As a future research, the implementation of the proposed solution can be studied in a hostile environment.

REFERENCES

[1] K. A. Varmedal, H. Klevjer, J. Hovlandsvåg, A. Jøsang, J. Vincent, and L. Miralabé, "The OffPAD: Requirements and usage," in *Network and System Security*. Berlin, Germany: Springer, 2013, pp. 80–93.
[2] J. Franks *et al.*, *HTTP Authentication: Basic and Digest Access Authentication*, document RFC 2617, Jun. 1999.
[3] C.-M. Huang and J.-W. Li, "One-pass authentication and key agreement procedure in IP multimedia subsystem for UMTS," in *Proc. 21st Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, May 2007, pp. 482–489.
[4] J. Antonysamy and S. K. Patro, "Multipurpose band specific antenna design and realization for wireless authentication device," in *Proc. Indian Antenna Week (IAW)*, Dec. 2011, pp. 1–4.
[5] J. Wang, S. Lian, and G. Liu, "On the analysis and design of secure multimedia authentication scheme," in *Proc. 3rd Int. Conf. Commun. Netw. China (ChinaCom)*, Aug. 2008, pp. 1298–1302.
[6] B. Huang, M. K. Khan, L. Wu, F. T. B. Muhaya, and D. He, "An efficient remote user authentication with key agreement scheme using elliptic curve cryptography," *Wireless Pers. Commun.*, vol. 85, no. 1, pp. 225–240, 2015.
[7] S. Kumari, M. K. Khan, and M. Atiquzzaman, "User authentication schemes for wireless sensor networks: A review," *Ad Hoc Netw.*, vol. 27, pp. 159–194, Apr. 2015.
[8] D. He, C. Chen, S. Chan, and J. Bu, "Analysis and improvement of a secure and efficient handover authentication for wireless networks," *IEEE Commun. Lett.*, vol. 16, no. 8, pp. 1270–1273, Aug. 2012.
[9] D. He, C. Chen, S. Chan, and J. Bu, "Secure and efficient handover authentication based on bilinear pairing functions," *IEEE Trans. Wireless Commun.*, vol. 11, no. 1, pp. 48–53, Jan. 2012.
[10] A. K. Das, "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards," *IET Inf. Secur.*, vol. 5, no. 3, pp. 145–151, Sep. 2011.
[11] Y. Seifi, S. Suriadi, E. Foo, and C. Boyd, "Analysis of two authorization protocols using colored Petri nets," *Int. J. Inf. Secur.*, vol. 14, no. 3, pp. 221–247, 2015.
[12] J.-K. Tsay and S. F. Mjølsnes, "A vulnerability in the UMTS and LTE authentication and key agreement protocols," in *Computer Network Security* (Lecture Notes in Computer Science), vol. 7531, I. Kotenko and V. Skormin, Eds. Berlin, Germany: Springer-Verlag, 2012, pp. 65–76.
[13] M. K. Khan, S.-K. Kim, and K. Alghathbar, "Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme,'" *Comput. Commun.*, vol. 34, pp. 305–309, Mar. 2011.
[14] M. Miculan and C. Urban, "Formal analysis of Facebook connect single sign-on authentication protocol," in *Proc. SOFSEM*, 2011, pp. 22–28.
[15] Y. Bang, D.-J. Lee, Y.-S. Bae, and J.-H. Ahn, "Improving information security management: An analysis of ID–password usage and a new login vulnerability measure," *Int. J. Inf. Manage.*, vol. 32, pp. 409–418, Oct. 2012.
[16] T. Li and R. Deng, "Vulnerability analysis of EMAP-an efficient RFID mutual authentication protocol," in *Proc. 2nd Int. Conf. Availability, Rel. Secur. (ARES)*, Apr. 2007, pp. 238–245.
[17] B. Cui, Z. Wang, B. Zhao, and X. Chen, "Design and analysis of secure mechanisms based on tripartite credibility for RFID systems," *Comput. Standards Interfaces*, vol. 44, pp. 110–116, Feb. 2016.
[18] M. H. Jahanian, F. Amin, and A. H. Jahangir, "Analysis of TESLA protocol in vehicular ad hoc networks using timed colored Petri nets," in *Proc. 6th Int. Conf. Inf. Commun. Syst. (ICICS)*, Apr. 2015, pp. 222–227.
[19] N. Ruan and Y. Hori, "DoS attack-tolerant TESLA-based broadcast authentication protocol in Internet of Things," in *Proc. Int. Conf. Sel. Topics Mobile Wireless Netw. (iCOST)*, Jul. 2012, pp. 60–65.
[20] P. Peris-Lopez, T. Li, T.-L. Lim, J. C. Hernandez-Castro, and J. M. Estevez-Tapiador, "Vulnerability analysis of a mutual authentication scheme under the EPC class-1 generation-2 standard," in *Proc. Workshop RFID Secur.*, 2008, p. 11.
[21] H. A. Dinesha and V. K. Agrawal, "Multi-level authentication technique for accessing cloud services," in *Proc. Int. Conf. Comput., Commun. Appl. (ICCCA)*, Feb. 2012, pp. 1–4.
[22] Q. Li and W. Trappe, "Reducing delay and enhancing DoS resistance in multicast authentication through multigrade security," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 2, pp. 190–204, Jun. 2006.
[23] R. Amin and G. P. Biswas, "A novel user authentication and key agreement protocol for accessing multi-medical server usable in TMIS," *J. Med. Syst.*, vol. 39, no. 3, p. 33, 2015.
[24] A. Plateaux, P. Lacharme, A. Jøsang, and C. Rosenberger, "One-time biometrics for online banking and electronic payment authentication," in *Availability, Reliability, and Security in Information Systems* (Lecture Notes in Computer Science), vol. 8708. Berlin, Germany: Springer-Verlag, Sep. 2014, pp. 179–193.
[25] E. Sano *et al.*, "Fingerprint authentication device based on optical characteristics inside a finger," in *Proc. Conf. Comput. Vis. Pattern Recognit. Workshop (CVPRW)*, Jun. 2006, p. 27.
[26] X. Huang, Y. Xiang, E. Bertino, J. Zhou, and L. Xu, "Robust multi-factor authentication for fragile communications," *IEEE Trans. Depend. Sec. Comput.*, vol. 11, no. 6, pp. 568–581, Nov./Dec. 2014.
[27] M.-S. Hwang and L.-H. Li, "A new remote user authentication scheme using smart cards," *IEEE Trans. Consum. Electron.*, vol. 46, no. 1, pp. 28–30, Feb. 2000.
[28] J. Prieto, "Strong personal authentication scheme using mobile technology," in *Proc. IN3 Working Paper Ser.*, 2003, pp. 1–14.
[29] R. Lindemann, "The evolution of authentication," in *ISSE Securing Electronic Business Processes*, H. Reimer, N. Pohlmann, and W. Schneider, Eds. Springer Vieweg, 2013, pp. 11–19.
[30] Y. Lee, G. Y. Lee, H. J. Kim, and C. K. Jeong, "Performance analysis of authentication and key distribution scheme for mobile multi-hop relay in IEEE 802.16 j," *Pers. Ubiquitous Comput.*, vol. 16, no. 6, pp. 697–706, 2012.
[31] W. Jeon, J. Kim, Y. Lee, and D. Won, "Security analysis of authentication scheme for wireless communications with user anonymity," in *Information Technology Convergence, Secure and Trust Computing, and Data Management* (Lecture Notes in Electrical Engineering), vol. 180, J. Park, J. Kim, D. Zou, and Y. Lee, Eds. Dordrecht, The Netherlands: Springer, Sep. 2012, pp. 225–231.
[32] M. Luo, Y. Wen, and H. Zhao, "An enhanced authentication and key agreement mechanism for SIP using certificateless public-key cryptography," in *Proc. 9th Int. Conf. Young Comput. Sci. (ICYCS)*, Nov. 2008, pp. 1577–1582.
[33] J. Clark and J. Jacob, "Attacking authentication protocols," *High Integr. Syst.*, vol. 1, pp. 465–474, Aug. 1996.
[34] H. Klevjer, K. A. Varmedal, and A. Jøsang, "Extended http digest access authentication," in *Policies and Research in Identity Management* (IFIP Advances in Information and Communication Technology), vol. 396, S. Fischer-Hübner, E. de Leeuw, and C. Mitchell, Eds. Berlin, Germany: Springer, Apr. 2013, pp. 83–96.
[35] K. Sameni, N. Yazdani, and A. Payandeh, "Analysis of attacks in authentication protocol of IEEE 802.16 e," *Int. J. Comput. Netw. Technol.*, vol. 1, no. 1, pp. 33–44, 2013.
[36] *TCG Specification Architecture Overview. TCG Specification Version 1.2*, Trusted Comput. Group (TCG), Portland, OR, USA, Apr. 2003.

[37] M. Alhaidary and S. M. M. Rahman, "Security vulnerability analysis and corresponding mitigation for password-based authentication using an offline personal authentication device," in *Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET)*, Chennai, India, Mar. 2016, pp. 842–849.
[38] L. Lamport, "The temporal logic of actions," *ACM Trans. Program. Langu. Syst.*, vol. 16, no. 3, pp. 872–923, 1994.
[39] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.
[40] M. S. Hossain, G. Muhammad, S. M. M. Rahman, W. Abdul, A. Alelaiwi, and A. Alamri, "Toward end-to-end biomet rics-based security for IoT infrastructure," *IEEE Wireless Commun.*, vol. 23, no. 5, pp. 44–51, Oct. 2016.

MADA ALHAIDARY received the master's degree from the Information Systems Department, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. She is currently a Researcher with the National Center for Cybersecurity Technologies, King Abdulaziz City for Science and Technology, Riyadh. Her research interests include cloud computing security, cryptography and authentication, multimedia security, and e-health.

SK MD MIZANUR RAHMAN received the Ph.D. degree in risk engineering (major in cyber security engineering) from the Laboratory of Cryptography and Information Security, Department of Risk Engineering, University of Tsukuba, Japan, in 2007. He is currently an Assistant Professor with the Information Systems Department, College of Computer and Information Sciences, King Saud University, Saudi Arabia. He was involved in cryptography and security engineering in high-tech industry in Ottawa, Canada, for several years. He was a Post-Doctoral Researcher with the University of Ottawa, University of Ontario Institute of Technology, and University of Guelph, Canada, for several years. He has published around 100 scientific articles in peer-reviewed renowned journals and conferences, including the IEEE TPDS, the IEEE Access, the IEEE WC, the IEEE *Communications Magazine*, the Elsevier FGCS, the Elsevier JPDC, the Wiley CCPE, the Wiley SCN, the Wiley WCMC, the *Multimedia Systems* (Springer), and the Springer *P2P Networking and Applications*. His research interest is in different domains of cybersecurity, cryptography and application security. Dr. Rahman received the IPSJ Digital Courier Funai Young Researcher Encouragement Award for his excellent contribution in IT security research from the Information Processing Society of Japan, and the Gold Medal for distinction marks in his undergraduate and graduate programs. He holds a U.S. patent on white-box implementation for an NIST Standard Key Exchange Protocol.

MOHAMMED ZAKARIAH received the master's degree in computer science. He is currently a Research Assistant and Lecturer with the Computer Science Department, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. He has published over 18 papers in various reputed ISI indexed journals in several fields of research. His research interest includes bioinformatics, image processing, speech processing, audio forensics cloud computing, and security.

M. SHAMIM HOSSAIN received the Ph.D. degree in electrical and computer engineering from the University of Ottawa, Ottawa, ON, Canada. He is currently a Professor with King Saud University, Riyadh, Saudi Arabia. He has authored and co-authored around 160 publications including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, books, and book chapters. His research interests include serious games, social media, IoT, cloud and multimedia for healthcare, smart health, and resource provisioning for big data processing on media clouds. He has served as a member of the organizing and technical committees of several international conferences and workshops. He is a member of the ACM and the ACM SIGMM. He was a recipient of a number of awards, including the Best Conference Paper Award, the 2016 *ACM Transactions on Multimedia Computing, Communications and Applications* Nicolas D. Georganas Best Paper Award, and the Research in Excellence Award from King Saud University. He has served as the co-chair, general chair, workshop chair, publication chair, and TPC for over 12 IEEE and ACM conferences and workshops. He currently serves as the Co-Chair of the 1st IEEE ICME Workshop on Multimedia Services and Tools for S-Health MUST-SH 2018. He served as a Guest Editor for the IEEE Transactions on Information Technology in Biomedicine (currently JBHI), the *International Journal of Multimedia Tools and Applications* (Springer), the *Cluster Computing* (Springer), the *Future Generation Computer Systems* (Elsevier), the *Computers and Electrical Engineering* (Elsevier), and the *International Journal of Distributed Sensor Networks*. He is on the Editorial Board of the IEEE Access, IEEE Multimedia, the *Computers and Electrical Engineering* (Elsevier), the *Games for Health Journal*, and the *International Journal of Multimedia Tools and Applications* (Springer). He currently serves as a Lead Guest Editor for the *IEEE Communication Magazine*, the IEEE Transactions on Cloud Computing, the IEEE Access, the *Future Generation Computer Systems* (Elsevier), and *Sensors (MDPI)*.

ATIF ALAMRI is currently an Associate Professor with the Information Systems Department, College of Computer and Information Sciences, King Saud University. Riyadh, Saudi Arabia. His research interests include multimedia-assisted health systems, ambient intelligence, and service-oriented architecture. He serves as a program committee member for many conferences in multimedia, virtual environments, and medical applications. He was the Co-Chair of the first IEEE International Workshop on Multimedia Services and Technologies for E-Health, and the Technical Program Co-Chair of the 10th IEEE International Symposium on Haptic Audio Visual Environments and Games. He has been a Guest Associate Editor of the IEEE Transactions on Instrumentation and Measurement.

MD SARWAR M HAQUE received the M.Sc. degree in computer systems and networking from the University of Greenwich, London, U.K. He is currently a Faculty Member with the King Fahd University of Petroleum and Minerals. He has published a number of peer-reviewed publications. He is also involved in several research and development projects. His research interest includes Internet of Things, network security and privacy, data mining and machine learning techniques, performance analysis and simulation of computer and communication systems, and image processing.

B. B. GUPTA received the Ph.D. degree in information and cyber security from IIT Roorkee, Roorkee, India. He has published over 90 research papers (as well as three books and 14 book chapters) in international journals and conferences of high repute, including the IEEE, Elsevier, ACM, Springer, and Wiley Inderscience. His research interest includes information security, cyber security, mobile security, cloud computing, Web security, intrusion detection, computer networks and phishing. He was a Visiting Researcher with Yamaguchi University, Japan, in 2015. He has visited several countries, such as Canada, Japan, China, Malaysia, and Hong Kong, to present his research work. His biography was selected and published in the 30th Edition of Marquis *Who's Who in the World* in 2012. He is also a principal investigator of various research and development projects. He is supervising ten students for their master's and doctoral research work in the area of information and cyber security. He has also served as a technical program committee member of more than 20 international conferences worldwide. He is member of the IEEE, the ACM, SIGCOMM, the Society of Digital Information and Wireless Communications, the Internet Society, the Institute of Nanotechnology, a Life Member of the International Association of Engineers, and a Life Member of the International Association of Computer Science and Information Technology. He is an editor of various international journals and magazines. He is serving as an Associate Editor for the IEEE Access, an Associate Editor for the IJICS and Inderscience, and an Executive Editor for the IJITCA and Inderscience. He is also serving as a Reviewer for journals of the IEEE, Springer, Wiley, and Taylor & Francis, and as guest editor of various reputed journals.