IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 26, 2018, accepted May 21, 2018, date of publication June 7, 2018, date of current version July 12, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2845299

Security Analysis of Smartphone and Cloud Computing Authentication Frameworks and Protocols

ZEESHAN SIDDIQUI[1], OMAR TAYAN[2], (Member, IEEE), AND MUHAMMAD KHURRAM KHAN[3]

[1]Modern College of Business and Sciences, Muscat 133, Oman
[2]Department of Computer Engineering and NOOR Research Center, College of Computer Science and Engineering, Taibah University, Madinah 41411, Saudi Arabia
[3] Center of Excellence in Information Assurance, King Saud University, Riyadh 11653, Saudi Arabia

Corresponding author: Omar Tayan (otayan@taibahu.edu.sa)

This work was supported by the King Abdulaziz City of Science and Technology during the academic year 2015/2016 under Grant 440-34-أـت".

ABSTRACT We live in a digital world where every detail of our information is being transferred from one smart device to another via cross-platform, third-party cloud services. Smart technologies, such as, smartphones are playing dynamic roles in order to successfully complete our daily routines and official tasks that require access to all types of critical data. Before the advent of these smart technologies, securing critical information was quite a challenge. However, after the advent and global adoption of such technologies, information security has become one of the primary and most fundamental task for security professionals. The integration of social media has made this task even more challenging to undertake successfully. To this day, there are plentiful studies in which numerous authentication and security techniques were proposed and developed for smartphone and cloud computing technologies. These studies have successfully addressed multiple authentication threats and other related issues in existing the smartphone and cloud computing technologies. However, to the best of our understanding and knowledge, these studies lack many aspects in terms of authentication attacks, logical authentication analysis, and the absence of authentication implementation scenarios. Due to these authentication anomalies and ambiguities, such studies cannot be fully considered for successful implementation. Therefore, in this paper, we have performed a comprehensive security analysis and review of various smartphone and cloud computing authentication frameworks and protocols to outline up-to-date authentication threats and issues in the literature. These authentication challenges are further summarized and presented in the form of different graphs to illustrate where the research is currently heading. Finally, based on those outcomes, we identify the latest and existing authentication uncertainties, threats, and other related issues to address future directions and open research issues in the domain of the smartphone- and cloud-computing authentication.

INDEX TERMS Smartphone, remote user authentication, authentication protocols, three-factor authentication, BAN logic, cloud computing.

I. INTRODUCTION

Modern day technologies are evolving from smartcards to more advanced and smart technologies such as Smartphones. Since 1968, smartcard based privacy and security challenges were addressed, with numerous proposals emerging on smartcard based authentication frameworks and protocols. However, due to the existing smartcard limitations, the security and privacy challenges were not completely addressed and presented [1]. On the other hand, Smartphones are playing a vigorous role to accomplish our daily tasks and routines. From waking-up to going-to-bed, every routine is now linked and performed with the help of Smartphone applications. Based on Web of Sciences citation analysis, the rising trend of Smartphone usage has made information security a more challenging task, and a consequent increase in research and citations in the past two decades (Figure 1). Additionally, with the advent and integration of Cloud Computing (CC) technologies, security and privacy issues have become more challenging. Our data, which was initially stored on our hard drives, is now mainly stored on third-party Cloud Servers.

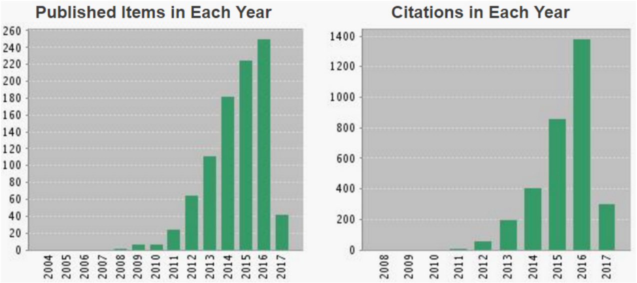

FIGURE 1. Publications and citations for smartphone usage research and trend.

Moreover, according to [3], 75% of Smartphone applications require access to critical user data, including Location, Device ID, Camera, Contacts etc. The use of those technologies has made Smartphones vulnerable to Smartphone-level security threats, and has increased susceptibility to third-part security threats [1].

There are numerous authentication frameworks proposed and developed for Smartphones to secure critical user information [4]–[10]. However, in the case of shared resources like CC, securing critical information is not a normal task due to its dependency on loosely coupled cloud resources. Consequently, built-in Smartphone authentication frameworks are not sufficient to provide verification and authentication of third-party CC resources [11]–[15], since in most cases the user also has to rely on the authentication mechanism provided by the CC resource. For example, once information is transferred from Smartphone to a cloud resource, the user has to completely rely on the authentication or security framework developed by that particular resource [16] and [17].

A. CONCEPTS OF SECURITY AND AUTHENTICATION

Nowadays, Smartphones are well equipped with numerous authentication mechanisms such as, Multiple Factor Authentication (MFA),Two Factor Authentication (2FA) and Three Factor Authentication (3FA) [18]–[20]. A 3FA based Smartphone is able to provide higher security for critical information [21]. However, it is not necessary that cloud resources (integrated within a Smartphone application) provide support for MFA or 3FA based authentication. Additionally, the risk of a security breach is higher when such cloud resources are involved in transferring user critical information and have access to built-in Smartphone resources (Figure 2). On the other hand, without such access permissions, those applications will fail to perform essential tasks associated with either daily routines or professional chores. Those risks are not only limited to Smartphones. Nowadays, Smart devices such as tablets and phone-tabs have replaced our regular Personal Computers and Laptops. Moreover, almost all domains and sectors are utilizing those smart technologies to perform their normal or critical operations [22] and [23]. The security risk is very high when we consider sensitive domains and sectors that include: Military, Defense, Telecommunications, Health and other governmental or non-governmental entities [24]–[29].

Based on the above understanding, multiple authentication frameworks and protocols are proposed and developed to provide end-to-end security, privacy and verification to all entities and domains. However, there remains plenty to cover and explore in terms of security and privacy in Smartphones and CC authentication frameworks. The purpose of this study is to analyze and document existing and primary security challenges pertaining to Smartphones and CC Authentication Frameworks and Protocols. The remainder of the paper is organized as follows: We provide a brief background on the basics of Authentication Protocols, its Factors and Analysis Methods in Section II. A detailed and comprehensive Literature Review is conducted in Section III by wrapping up multiple reviews of Smartphone and CC authentication frameworks and protocols. Section IV provides detailed analysis of the literature review and highlights a number of challenges with respect to security and privacy pitfalls and anomalies. Section IV also presents the summary of the literature with the help of different illustrative charts. Section V concludes this study and discusses future directions in the light of the challenges highlighted during the analyses of the literature review and the summary.

II. BACKGROUND

For improved understanding, we further expand on the relevant issues underlying authentication by discussing authentication protocols, factors and different analysis and verification methods involved in designing, developing, validating and implementing a digital authentication framework.

A. AUTHENTICATION PROTOCOLS

The purpose of an authentication protocol is to provide secure data exchange and communication between all the entities of a system using cryptographic digital rules [30]. An authentication protocol provides assurance of key agreements, undisclosed sharing, non-denial methods and multi-party computation [31]. Suchprotocols aim towards providing complete secrecy and preserve security in the presence of an attacker. It is highly irrelevant that an adversary must follow specific attack rules, attack patterns or characterization [32].

There are various authentication protocols which are used in modern day authentication frameworks,such as, Host Identity Protocol (HIP), OpenID Protocol, Password Authentication Protocol (PAP), Secure Remote Password Protocol (SRP) etc [33]–[36]. However, in authentication frameworks, SRP is the most widely used remote authentication protocol [37]–[39].

B. AUTHENTICATION FACTORS

A remote user authentication protocol comprises of a number of authentication factors. Moreover, in order to violate or compromise any protocol, an adversary has to map its attack on the communication leading to the successful authentication of those authentication factors [32]. Such authentication factors are recognized by international security standardization bodies [40] and [41] and include:

1 Something the User Knows, e.g., username/password. This authentication factor is widely known as First Authentication Factor or 1FA [42].
2 Something the User Is, e.g., user biometrics. This authentication factor is widely known as Second Authentication Factor or 2FA [43].
3 Something the User Has, e.g., a mobile device. This factor is widely known as Third Authentication Factor or 3FA [44].

Three-factor or multi-factor authentication is a generalized term based on the number of authentication factors considered to be implemented in any authentication framework. The choice and implementation of those authentication factors are based on the existing requirements of the particular framework, whether it is a Smartphone or Smartcard based framework. Authentication frameworks which comprise of two or more factors of authentication are considered as three-factor or multi-factor authentication frameworks. Before the advent of Smartphones, digital transactions were highly dependable on Smartcards. However, Smartphones are yet to be considered as a successful replacement of Smartcards. This is due to the fact that Smartcards are still playing vital role in digital transactions and there are several multi-factor authentication frameworks being proposed and implemented to improve Smartcard based authentication frameworks. It is a well-known fact that Smartphones are more advanced and capable in comparison with their Smartcard counterparts. Authentication frameworks proposed and implemented for Smartphones are significantly more advanced and capable as compared to the authentication frameworks proposed for Smartcards. In comparison with Smartcard authentication frameworks, several studies have successfully proposed and implemented numerous highly functional, robust and highly secure Smartphone based multi-factor authentication frameworks. Those studies were not only proposed and implemented, but were successfully verified, validated and compared with the existing and previous Smartcard based multi-factor and three-factor authentication frameworks.

Moreover, the advent of the Smartphone has witnessed the emergence of cloud computing as a new concept that could integrate with Smartphone technology and offers a range of powerful services including processing power and storage. In contrast, Smartcards did not integrate well with cloud computing frameworks, and Smartcard authentication frameworks would not store sensitive credentials on cloud servers. Since the advent of cloud computing, the cloud computing infrastructure has enhanced its security and privacy capabilities, and hence, numerous Smartphone based multi-factor authentication frameworks were successfully proposed and developed for integration with cloud computing as compared to Smartcard based authentication frameworks. This is again due to the fact that a Smartphone based cloud computing infrastructures offer advanced functionalities and capabilities as compared to Smartcard based authentication frameworks.

Recently, authentication studies have utilized three-factor and multi-factor authentication to develop resilient authentication protocols for their different systems. However, such authentication factors are also exploited by adversaries in every sector, such as, healthcare, military, e-commerce/banking etc. in order to gain access to the authentication frameworks [45]–[48]. A compromise of the authentication factors may occur due to several reasons, such as; privacy disclosures, sensitive data storage at the user-end, loss of identities and operational interruptions [49]–[51], [71]. Any level of compromise in the authentication factors results in vulnerability towards numerous authentication attacks such as; impersonation attacks [52], parallel processing attacks [53], replay attacks [54], password guessing attacks [55], insider attacks [56], DOS attacks [57], forgery attacks [58], server-spoofing attacks [52] and reflection attacks [59].

C. FORMAL ANALYSIS AND VERIFICATION METHODS

Authentication protocols developed using known authentication factors are being analyzed and improved on a continuous basis. Researchers are analyzing existing protocols using numerous methods and techniques to redevelop more concrete authentication protocols which are robust and secure against modern authentication attacks [55], [60], [61]. In order to analyze authentication protocols, numerous formal methods, techniques and tools are utilized. For logical analysis and verification of an authentication protocols, Burrows Abadi Needham (BAN) Logic [62] and Syverson Van Oorschot (SVO) Logic [63] are widely used. For automated security testing, ProVerif [64] and Scyther [65] are generally used. However, in the majority of the studies, cryptanalysis [66] is considered, which involves a manual *threat-by-threat* analysis of an authentication protocol. We now describe three formal methods that are normally utilized to achieve authentication verification and validation.

1) BAN LOGIC

In 1989, Burrows *et al.* proposed and presented a formal logical analysis method in order to verify a security protocol. The method is nowadays very widely used and known as BAN logic [62]. BAN logic works in three steps while providing the user the ability to evaluate and analyze any protocol. The formal steps are; analyzing the assumptions, verify the goal and acquiring the goal (through group of rules/postulates). The main objective of BAN logic analysis is to verify the message freshness throughout the communication. The BAN logical analysis method is considered the most widely and most effective method to analyze any authentication protocol [67]–[69].

2) SCYTHER

In 2006, Cremers and Casimier proposed an automated method known as Scyther to analyze any authentication protocol [65]. Scyther works on analyzing authentication factors.

An authentication communication is highly dependent upon the authentication factor being used. An adversary would then attempt to compromise the authentication communication in order to obtain the associated authentication factors involved. For example, if an adversary has control or knowledge of a session variable involved in the communication, then he/she would attempt to obtain the 1FA, 2FA or 3FA of a particular entity involved in the communication to gain access to the system. Therefore, it is required and highly recommended to verify the authentication factors involved in an authentication protocol. Scyther is one of the best available methods for this purpose. The role of Scyther is to initially transform an authentication protocol into Scyther readable code. After successful transformation, it highlights the authentication goals and further runs the tracing on the *to-and-fro* communication based on the authentication factors. A similar number of tracing-runs is verified and tested against all authentication factors involved in an individual protocol. Therefore, the tests are repeated on each and every user communication [65] and [70].

3) CRYPTANALYSIS

Cryptanalysis is used to breach a cryptographic or authentication protocol by applying mathematical calculations to study its concealed aspects. It is considered the most effective manual *threat-by-threat* analysis performed on computational authentication protocols. For successful cryptanalysis, it is mandatory to possess ground knowledge of the computations being used in an authentication protocol which is required to be verified or analyzed. Cryptanalysis is being successfully used in a number of studies such as [38], [39], [55], and [66].

4) AUTHENTICATION PROPERTIES

An authentication protocol is considered to be verified when it completely satisfies the authentication properties of the formal method being used. Regardless of whatever method being considered, there are several security properties a protocol should satisfy to be considered as highly secure. Some of those properties are; Message Verification, Nonce Rule Verification, Authority Rule Verification, Message Freshness, Message Aliveness and Message Secrecy [62].

5) PROVABLE SECURITY

Provable security is another formal analysis and verification approach that is considered to have an important role in the design and analysis of cryptographic systems [72], [73]. Essentially, provable security is used for proving that a cryptographic method is secure and is achieved by deriving formal definitions of security and applying techniques adopted from complexity theory and probability theory on the constituent cryptographic primitives from which they are constructed [73]. Degabriele *et al.* [73] and other studies have classified provable security in terms of two main branches: *perfect secrecy* and *semantic security*. The former method is used to confirm "perfect secrecy" for an encryption scheme that guarantees non-leakage of plaintext information. However, the key space required is as large as the plaintext space, which makes this method difficult for practical use. On the other hand, the latter method considers the bounded computational resources possessed by adversaries, and overcomes the practical deployment constraints in perfect secrecy. To date, semantic security is considered as the most widely applied form of provable security [72], [73].

A number of recent works can be found in the literature with the aim of provably satisfying particular security notions for various protocol implementations [72]–[74], [77]. A number of initial efforts in conceptualizing provable security of cryptosystems had included the earlier works by Goldwasser and Macali [75] and Bellare and Namprempre [76]. More recently, an analysis of two previous designs for realizing authenticated encryption in Kerberos version 5 was given in [72]. It was shown that one of the designs being analyzed had not provided integrity given that the constituents' constructs/functions were proven secure. Boldyreva and Kumar [72] had then proposed design modifications which provide provable privacy and authentication when secure constituent constructs are used. Degabriele *et al.* [73] apply provable security for analyzing symmetric encryption schemes used in Internet Protocol Security (IPSec), Secure Sockets Layer (SSL)/Transport Layer Security (TLS) and Secure Shell (SSH) protocols. In their analyses of those protocols, [73] had explained that previous proofs had not completely captured all the subtle details and practical deployment factors that are not normally considered in formal analyses. Consequently, those previous proofs being analyzed were only considered valid for a subset of attack types. Odelu *et al.* [74] had analyzed an authenticated key agreement proof for smart grids, explaining that the previous scheme had failed to achieve credential's privacy and session-key security in a Canetti-Krawczyk adversary model. The authors had then proposed and analyzed a new provable secure authenticated key distribution approach using the same adversary attack model for smart grids; describing that their proof had overcome the deficiencies of the previous proof in terms of the investigated security functionalities.

A review of the literature had evidenced the extensive use of provable security in the domain of cryptographic systems. However, it was noted that provable security has also been associated with a significant limitation in the degree of confidence of developed proofs. For instance, many recent studies have discovered attacks on cryptographic schemes previously proven as secure [72]–[73], [77]. In particular, many security proofs and notions were conditional upon their constituent sub-functions and underlying assumptions used. Additionally, formal analyses may not accurately represent the real-life computational capabilities of an adversary or may not capture implementation-specific attacks within the scope of the security model. Protocols that provide programmer-flexibility or optional implementation constructs (that lack detailed implementation guidance) may provide a source of vulnerability and attract new implementation-specific attacks. Hence, it is important that cryptosystem designers apply provable security proofs with caution and understanding of the scope and validity for which the implementation accurately relates to the provably secure model.

III. LITERATURE REVIEW

This section covers a detailed and critical review of the pertinent and relevant literature based on the aim and objectives of this study. This review provides a detailed discussion of the present gap found in Smartphone and CC authentication frameworks and protocols. It is noted that authentication protocols for Smartphones as considered here relate to the authentication protocols and mechanisms specifically designed for the characteristics of Smartphone platforms and their usage, such as NFC mobile-authentication and one-time passwords (OTPs) sent to a user's mobile and are found in some e-banking applications (e.g. 3FA), whereas normal/traditional authentication protocols relate to mechanisms for accessing web-based and PC based applications as with an email username and password, for instance (e.g. 1FA). Biometrics or 2FA-schemesare examples of authentication mechanisms widely used in Smartphone authentication (e.g. in fingerprint scans) as well as traditional authentication (e.g. in facial-scan attendance records).

Section III-A provides details of current Smartphone based studies and authentication issues in various domains such as e-commerce, while Section III-B discusses the current authentication loopholes, authentication attacks and performance issues in the CC-based authentication frameworks and methods.

A. SMARTPHONE BASED AUTHENTICATION FRAMEWORKS AND PROTOCOLS

This section discusses Smartphone based authentication studies in which MFA, 2FA and 3FA authentication frameworks and protocols were proposed and implemented.

1) PERFORMANCE ANALYSIS OF TOUCH-INTERACTION BEHAVIOR FOR ACTIVE SMARTPHONE AUTHENTICATION

Recently, a reliability and applicability analysis of the user touch behavior for Smartphone-authentication has been investigated. Dynamic and static features were examined for user touch characterization. Several classification techniques were applied on the features for active authentication. Nearly 71 participant's data of around 134 900 touch operations were analyzed to judge the operational performance. Equal error rates were achieved between 1.72% and 9.01% with an operational length of 11 [78].

2) BEHAVIORAL BIOMETRICS AUTHENTICATION FOR SMARTPHONE DEVICES

Behavioral authentication and their risks were discussed by A. Alzubaidi *et al.* for the case of stolen or apprehended Smartphones. Numerous approaches and mechanisms, including continuous-authentication, were analyzed for behavioral biometrics based on different methodologies, datasets and assessment approaches. The study concluded with multiple directions within behavioral biometric authentication. Suggestions included; the ease of use while focusing on multiple characteristics and user behavior measurement during the application usage [79].

3) ENERGY EFFICIENT AUTHENTICATION FOR SMARTPHONE DEVICES

An energy-efficient, secure and fast authentication technique is proposed for intriguing Smartphone and cloud computing by Gasti *et al.* [80]. The authors' claimed that the current continuous-authentication and privacy protocols were not maintainable for Smartphones. The proposed work was evaluated with experimentation. The authors claimed that their authentication technique had resulted with only0.2 mWh, which is a negligible portion of the Smartphone battery. In [80], it was also claimed that the proposed protocol executed in 7.2s and 2s, for biometrical features with size 8 and 28, respectively. The humming distance is also calculated in 3.29 s in comparison with the Whitewash computation protocol of 95.57 s. The study concludes with the claim of being the only study providing continuous and low-latency authentication. However, the proposed protocols were only verified through manual security analysis and are not supported with validation and verification using authentication or cryptographic protocol validation methods, tools and techniques [80].

4) SMARTPHONE BASED DIGITAL IDENTITY AUTHENTICATION

A user centric mobile Identity Management (IDM) authentication protocol framework is proposed. The study in [82] has evaluated several IDM approaches and authentication types with available mobile IDM solutions. The proposed open mobile IDM framework is based on profile and context management, features including; preferences, time, location, status etc. There are several authentication and implementation limitations in the proposed IDM security framework. Several research areas considered had included: mobility, preferences, adaptability, services, profile management, authentication and network. The proposed solution had addressed only a few of those areas such as; generalized authentication framework and network integration. Regardless of the proposed authentication mechanism, the study lacks the use of a standardized verification analysis. Additionally, the authors of this study identified the implementation issues and drawbacks with respect to user preferences, QoS management, and service discovery and context awareness. Moreover, an authentication mechanism was proposed, but included no details of the computations used in the authentication protocols. Therefore, the IDM framework still requires a longer time frame to provide complete security validation of each and every research area involved [82].

5) ANDROID MOBILE PAYMENT AUTHENTICATION FRAMEWORK

A 3FA Smartphone mobile payment based on Android phones was presented in [83]. The scheme features 3FA

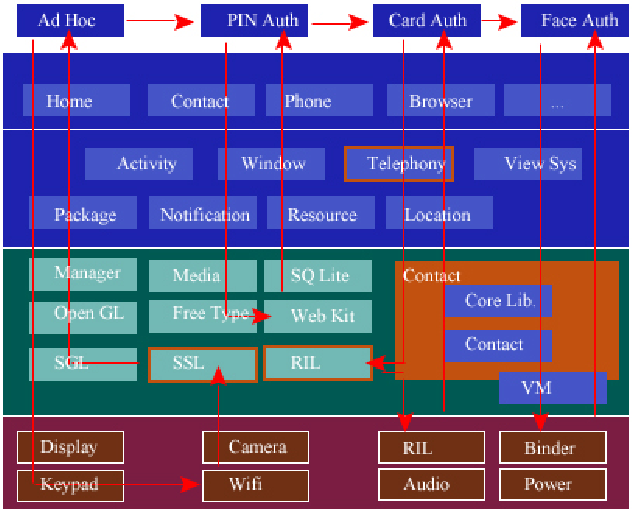

FIGURE 2. Implementation framework [83].

authentication blending biometrics, OTP and USIM together. The authentication mechanism was based on the HTTPS channel over Ad-hoc networking. Figure 2 illustrates the interface between the Android and Smartphone system components with the components of the proposed authentication framework. However, there were many issues present in this study. For instance, the use of HTTPS is not at all assumed to be completely secure. This is due to the fact that the authors fail to provide specific HTTPS attack analysis. Additionally, crucial information was stored in the mobile device, which is highly vulnerable in-case of theft or loss of the device. This leads to impersonation and offline password guessing attacks. In addition to authentication loopholes, the framework has performance issues. The Ad-Hoc connectivity had utilized 15 functional operations (15*fo*) between Database, Reader and Payers, which results with lower performance of the framework. The framework had utilized AES/DES/3DES which itself is vulnerable to cold-boot attacks. Those issues should be covered in order to consider this study for further implementation [83].

6) 2FA SCHEME FOR BANKING PAYMENT SYSTEM

In 2013, Günther and Borchert [84] proposed a Smartphone based online banking system enabled with NFC equipped bank cards. The proposed system involved a PC browser equipped with 2D barcode which is readable through the user Smartphone, which in return contacts the NFC enabled bank card using mobile NFC equipment. The NFC-TAN method was used in order to contact the NFC enabled debit card which allows the user to contact the device offline. The framework comprises of four phases, namely, login, scan, transaction and transfer. Figure 3 illustrates the simplicity of the proposed scheme and the relatively few components/entities involved. It was noted that NFC-TAN was vulnerable to the Man-in-the-Middle attack [84].

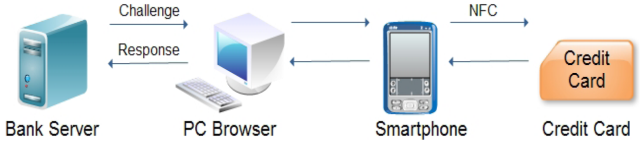

FIGURE 3. Payment scheme steps [84].

7) SMARTPHONE SECURITY SERVICE ON CLOUDS

Urien and Piramuthu [88] proposed a new concept of Cloud Secure Element (CoSE) for a Near Field Communication (NFC) based application in Smartphones for mobile payments. The proposed mechanism consists of four components, namely; service kiosk, Smartphone, grid or cloud of secure elements and an administration console. The authors further explained the complete workings of those components. The authors of this article claimed that their study has prevailed a number of security attacks including; relay attacks, DoS attacks and message modification attacks. However, they failed to provide any level of authentication attack analysis supported by any standardized technique. Therefore, this concept is insufficient to be considered for adoption [88].

B. CLOUD COMPUTING BASED AUTHENTICATION FRAMEWORKS AND PROTOCOLS

This section discusses CC based authentication studies in which MFA, 2FA and 3FA authentication frameworks and protocols were proposed and implemented.

1) PRIVACY-AWARE MOBILE CLOUD COMPUTING AUTHENTICATION

In the proposed authentication scheme by [81], Tsai and Lo presented a scheme that reduces the authentication processing time which is required for computation and communication among different clouds and third-party services. The proposed work is based on a single private key based authentication scheme. A dynamic nonce generation with bilinear cryptosystem is proposed which is claimed to be the primary strength of this proposed scheme. The authors claimed to achieve mutual authentication, user anonymity, key exchange and non-traceability of the user. They also claim that in case of scheme adoption, no verification tables are required for the card generator service and cloud computing service. However, the authors did not use logical authentication verification and validation methods/tools to verify and validate their schemes. Moreover, the implementation scenario and experimental work was never discussed for the provision of potential implementation of the proposed authentication scheme [81], [103].

2) CLOUD COMPUTING 2FA SECURE PROTECTION BETWEEN USER AND MOBILE

In this algorithm, Honggang *et al.* [85] discussed a 2FA secure watermarking sharing protocol that addresses several ongoing security issues in mobile cloud computing. The authors' introduced a new technique to tolerate multimedia errors of transmission joint watermarking and codes of *Reed-Solomon*. The main authentication issue in this study was the use of an information transporter during image watermarking. The authors did not utilize a random number during image counting. Due to this issue, the login phase of this study was vulnerable to parallel processing attacks [85], [104].

3) MOBILE CLOUD COMPUTING WITH BIOMETRIC AUTHENTICATION

In this biometric authentication protocol, Rassan and AlShaher [86] have proposed a new user security mechanism for Mobile Cloud Computing. Fingerprint recognition is used as a third factor by utilizing a Mobile phone. The fingerprint recognition algorithm is proposed which takes the imprint of the biometric image, converting the RGB to Grayscale, Normalizing and reducing the Blur effect and Segmenting the image for biometric authentication. The experiments were carried out along with functionality and performance testing. The experiments and results were carried out using Galaxy S3 and Blackberry *Z* Smartphones which shows that the proposed scheme performs well and easy in functionality. There are certain authentication points that require immediate remediation in this work. In addition, there is the absence of authentication computations, which always makes the work less adaptable. There is no identification that the image communication is taking place in plain text or not. Additionally, after the image imprint and before the conversion, the protocol or framework fails to provide a secure storage mechanism. Therefore, the authentication flow is vulnerable to parallel session attacks [86].

4) CLOUD BASED MFA BIOMETRIC AUTHENTICATION

In another study, Ziyad and Kannammal [87] have proposed a multifactor biometric authentication system for a CC environment. Palm vein and fingerprint features are adopted and handled for Smartcard based authentication. The data is matched using a *Match-On-Card* method which is completely stored on a Smartcard. The authentication process is subdivided in to registration and verification methods. The main authentication loophole was the storage of sensitive information within a smartcard. Therefore, in case of loss or theft, the information is vulnerable to impersonation and offline password guessing attacks [87].

5) CLOUD COMPUTING FRAMEWORK FOR ENHANCED MOBILE HEALTH

Another study is presented while proposing a Cloud Computing framework using a mobile device [89]. The framework was designed to introduce a CC framework comprising of healthcare services in mobile devices. The framework is focused on relieving mobile devices to use their computational resources for security and performance algorithms of the healthcare applications and services. The framework is built using Next Generation Networks (NGN) and IP Multimedia Subsystems (IMS). This work is not enough mature enough to present security roles for the registered users. The complete authentication framework is dependent on external providers which do not provide a clear approach in handling external authentications [89], [105].

6) CLOUD-BASED MOBILE SYSTEM FOR BIOMETRICS

A handwritten password biometric authentication system is presented in a CC environment [90]. The k-nearest neighbor and artificial neural network algorithms were used for recognition of each character. Combination methods based on parallel classifiers were utilized for error rate computations and recognition. The proposed system architecture is illustrated in Figure 4, which shows the phases and entities involved in the authentication process. This work enrolls the user ID based on touch-screen handwritten input, which makes this framework vulnerable to shoulder surfing attacks. Additionally, the pre-processing conversion is not secured or hashed before conversion. Hence, an adversary can easily launch a parallel processing attack to fetch and alter the ID in the pre-processing phase [90].

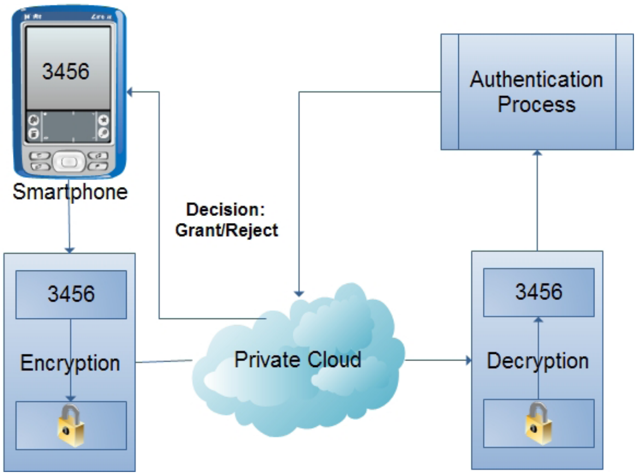

FIGURE 4. Handwritten cloud computing security framework [90].

7) DYNAMIC CREDENTIALS GENERATING PROTOCOL IN MOBILE CLOUD

Another study was conducted in 2013 at the University of Malaya [91]. In this study, the authors have proposed an enhanced and advanced credentials scheme which is dynamic in nature and based on a mobile cloud computing environment. The proposed system architecture comprises of a cloud service provider, and client organizations comprise of mobile phones, users and a managing database. The tests conducted were, time and consumption with two scenarios. This protocol utilizes *t1* and *t2* session variables which are open to parallel processing attacks due to no validation. Additionally, at the manager transfer process phase, the ID is in plain-text format which makes this protocol vulnerable to impersonation attacks [91].

8) SECURITY OF THE DATA BETWEEN CLOUD AND MOBILE DEVICE

Recently, Al-Hasan *et al.* [92] presented a secure approach for user authentication between a cloud and mobile phones. The level of security management is handled by the network providing companies and GPS. Public and private key algorithms are utilized in the proposed framework. The analysis in this article claims that the cryptographic key agreement on both sides (client/server) is secure. However, this claim is not at all supported with any standardized analysis in the light of modern day authentication attacks. The keys are stored and saved at the user end, which makes this protocol vulnerable to impersonation attacks [92], [106].

9) THEORETICAL AUTHENTICATION FRAMEWORK FOR TELEHEALTH

A Telehealth theoretical framework was proposed and presented in order to design and develop a secure health application [93]. The framework comprises of three prepositions; (1) Navigability, (2) Intrinsic Motivation and (3) Health Behaviors. The framework emphasized more on the level of Telehealth and its sub-systems. The system is distributed into five layers, namely, Healthcare Ecosystem, Healthcare Organization, Telehealth System, Entities Subsystem and Components. However, the security is not just the primary target of this framework, as the emphasis was more on wireless connectivity.

Table 1 summarizes the above reviews from the Smartphone and CC-based literature. In Table 1, emphasis is laid on a number of key evaluation metrics used throughout this study that includes: security analysis, performance analysis, validation analysis and implementation analysis. First, the 'security analysis' aspect relates to whether the study had investigated the impact of attack scenarios on the proposed scheme. Second, 'performance analysis' relates to the whether the study had included a performance evaluation of the proposed scheme, using metrics such as computational-time and memory-storage requirements. Next, the 'implementation-analysis' relates to whether the proposed scheme was actually implemented, with relevant observations being documented. Finally, the 'validation analysis' aspect describes a test-report documented following the application of automated and standard validation and verification tools on the proposed scheme.

IV. LITERATURE REVIEW ANALYSIS

In this section, the findings and analysis of the literature review is discussed. In Section III-A, the focus was on studies related to Smartphone authentication frameworks and protocols. In Section III-B, studies related to CC based authentication methodswere presented and their weaknesses were discussed in detail. Henceforth, theliterature review has provided a discrete survey of the current authentication protocols and factors in the Smartphones and CC domains. The detailed

TABLE 1. Summary of literature review.

Reference	**Security Analysis**	**Performance Analysis**	**Validation Analysis**	**Implementation Analysis**	**Mode**
Shen et al. (2016)[78]	Yes	Yes	No	No	Smartphone
Alzubaidi et al. (2016) [79]	Yes	No	No	Yes	Smartphone
Gasti et al. (2016)[80]	Yes	Yes	No	Yes	Smartphone
En-Nasry et al. (2011)[82]	Yes	No	No	No	Smartphone
Hu et al. (2012)[83]	No	No	No	No	Smartphone
Gunther et al. (2013)[84]	Yes	No	No	No	Smartphone
Urien et al. (2014)[88]	No	Yes	No	No	Smartphone
Tsai et al. (2015)[81]	No	Yes	No	No	Cloud Computing
Honggang et al. (2014)[85]	Yes	No	No	No	Cloud Computing
Rassan et al. (2014)[86]	Yes	Yes	No	Yes	Cloud Computing
Ziyad et al. (2014)[87]	No	No	No	No	Cloud Computing
Dinh et al. (2013)[89]	No	Yes	No	No	Cloud Computing
Omri et al. (2013)[90]	Yes	Yes	No	No	Cloud Computing
Khan et al. (2013)[91]	Yes	No	No	Yes	Cloud Computing
Al-Hasan et al. (2013)[92]	No	Yes	No	No	Cloud Computing
Sundar et al. (2012)[93]	Yes	Yes	No	No	Cloud Computing

findings of the literature review and some of the security deficienciesfound are now discussed below:

A. SECURITY ISSUES IN SMARTPHONE BASED STUDIES

In Section III-A, a detailed literature review was given of the studies based on Smartphone authentication frameworks and protocols. Now, we highlight some of the main findings and deficiencies related to the Smartphone based studies.

Firstly, mobile CC with a biometrics scheme is proposed in [86]. This study provided a generalized overview, but failed to present details of the authentication computations. Absence of a secure mechanism has made this study vulnerable to parallel processing attacks. Secondly, an NFC-based CC proposal was discussed in [88]. The proposal has outlined number of authentication attacks, however, the authors failed to explain how their work is sustainable to those attacks. Next, an advanced mobile based credential protocol is presented in [91]. The session variables, $t1$ and $t2$, used in this protocol are not secured, which makes it vulnerable to parallel session attacks.

Following a detailed and careful review of many Smartphone based authentication frameworks and protocols,the following authentication anomalies are now outlined:

- Absence of User Security Roles
- Service Discovery by Adversaries
- Client Side Storage of Credentials
- Absence of Randomization
- Plain-text Storage and Processing of Information
- Absence of Authentication Attack Analysis
- Vulnerable Session Variables
- Implementation and Validation Issues

Due to the aboveauthentication ambiguities, the following list now summarizes the authentication attacks found in those studies:

- Man-in-the-Middle Attacks
- Parallel Processing Attacks
- Impersonation Attacks
- Online/Offline Password Guessing Attacks
- Denial-of-Service Attacks
- Shoulder Surfing Attacks

B. SECURITY ISSUES IN CLOUD COMPUTING BASED STUDIES

In Section III-B, a detailed literature review was given on the studies based on CC authentication framework and protocols. Now, we highlight some of the main findings and deficiencies related to the CC based studies.

First, an MFA biometrics scheme for CC is presented in [87]. Palm based authentication is adopted using a smartcard. This protocol has loss of identity ambiguities which has made it vulnerable to impersonation and offline password guessing attacks. Next, a CC framework is discussed for Mobile Healthcare in [89]. The security model is only presented at a generalized level. The main authentication issue in this framework was the complete absence of user defined authentication roles. Additionally, in case of new services, the framework is dependable on external providers, with no external authentication scenarios being discussed. A cloud based mobile biometric framework is introduced in [90] using artificial neural networks. This framework has authentication issues at its pre-processing stage, where the information is stored in plain text, which makes the framework vulnerable to parallel processing attacks. In [91], an advanced mobile based credential protocol is presented. The session variables, $t1$ and $t2$, used in this protocol were not secure, which makes it vulnerable to parallel session attacks.

Following a detailed and careful review of many CC authentication frameworks and protocols, the following authentication anomalies are now outlined:

- Storage of sensitive data within smartcards
- Loss or theft of smartcards
- Identity loss during authentication
- Eavesdropping during registration
- Operation interruptions or operational errors

Due to the above authentication ambiguities, the entire authentication framework and its authentication protocols are vulnerable to numerous authentication attacks. A list of authentication attacks revealed following the review of authentication frameworks and protocols included:

- Insider Attacks
- Impersonation Attacks
- Replay Attacks
- Online/Offline Password Guessing Attacks
- Parallel Processing Attacks
- Denial-of-Service Attacks
- Forgery Attacks
- User/Server Anonymity Attacks

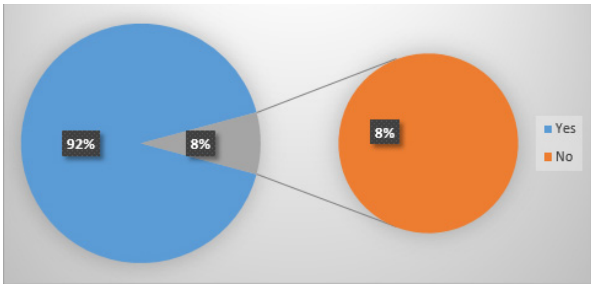

FIGURE 5. Impersonation attack analysis.

Summary: Figures 5 – 11 present a detailed vulnerability analysis of Smartphone-based studies reviewed, while Figures 12 – 19 present a detailed vulnerability analysis of the CC-based studies reviewed. Figures 5 – 9 and 12 – 16 show the ratio of studies that had evaluated the robustness and vulnerability of their respective schemes against common attack scenarios that include; impersonation attacks, insider attacks, online/offline attacks, replay attacks and parallel-processing attacks (as part of our security analysis). On the other hand, Figures 10 and 11 and Figures 17 - 19 illustrate the findings that relate to the performance analysis, implementation analysis and validation analysis from the related works.

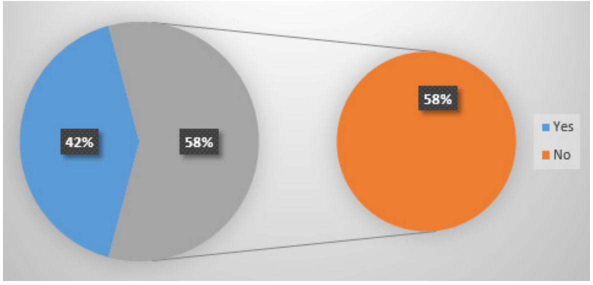

FIGURE 6. **Insider attack analysis.**

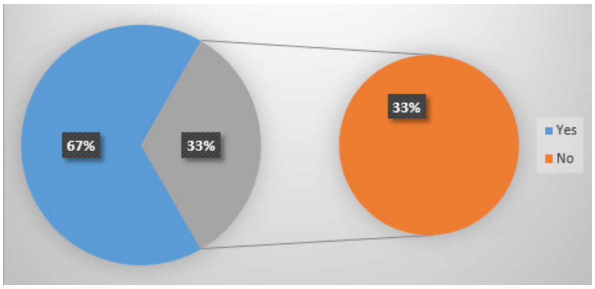

FIGURE 7. **Online/offline analysis.**

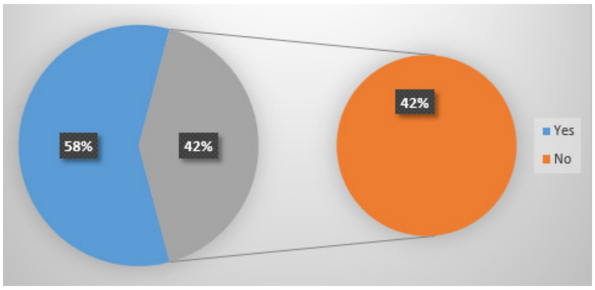

FIGURE 8. **Reply attack analysis.**

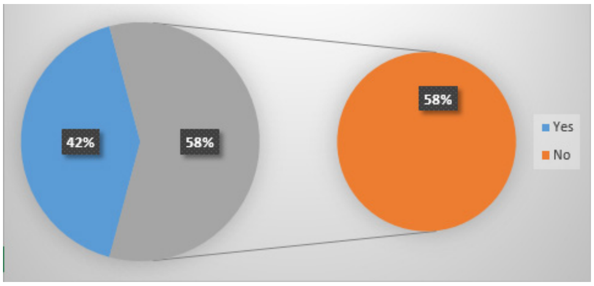

FIGURE 9. **Parallel processing attack analysis.**

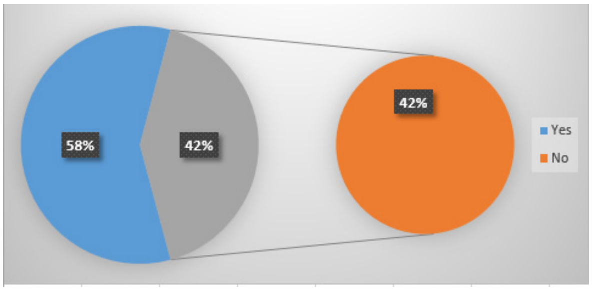

FIGURE 10. **Implementation analysis.**

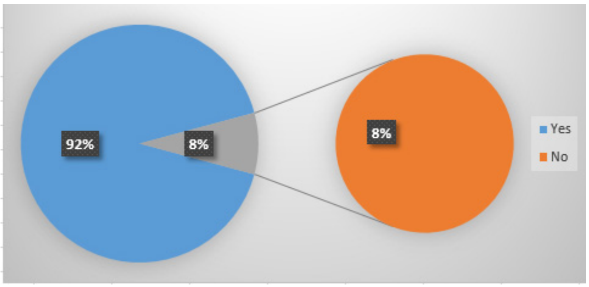

FIGURE 11. **Validation analysis.**

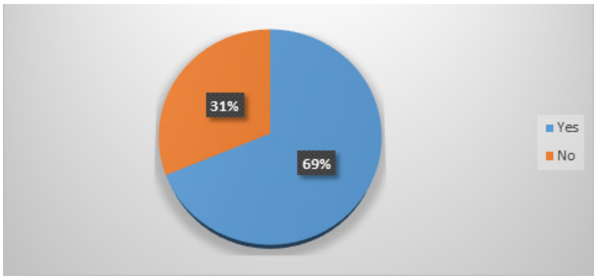

FIGURE 12. **Impersonation attack analysis.**

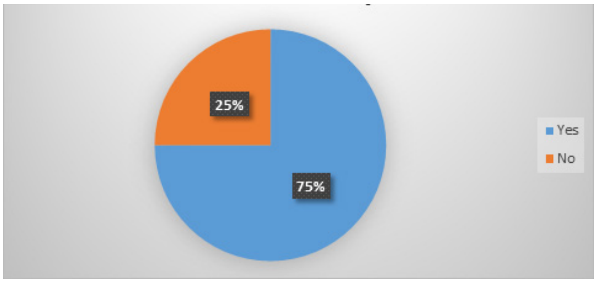

FIGURE 13. **Online/offline password guessing attack analysis.**

The analysis clearly shows that 92% of those studies are vulnerable to impersonation attacks (Figure 5), and 42% of studies are effected and insecure against insider attacks (Figure 6). Moreover, offline/online password guessing attacks and reply attacks are 67% and 58% respectively (Figures 7-8), along with parallel processing attacks which are 42% (Figure 9). Other than security and authentication vulnerabilities, those frameworks and methods also lack in performance, implementation, and validation limitations. In addition, it was observed that 83% of those studies possess serious performance issues, with 58% suffering from implementation limitations (Figure 10) and 92% were lacking in the use of validation and verification standards (Figure 11).

In Figure 12, it is shown that 69% of the current authentication schemes are found to be vulnerable to impersonation attack. Figure 13 illustrates that 75% of authentication

TABLE 2. Qualitative analysis of existing works in terms of key evaluation metrics.

Platform	Reference / Citation	Practicality / Efficiency	Comments on Security Level	Functionality
Smartphone	[80]	Energy-efficient and low-latency scheme	Only manual security analysis was performed with no automated validation	Energy-efficient authentication
	[82]	Applies a flexible concept through the use of an open IDM framework based on profile and management features	Proposed framework lacks the use of standard verification analysis, with many other implementation issues and drawbacks	Digital Identity Authentication using an open mobile IDM framework
	[83]	Support only for Android platform. Combines features of 3FA, biometrics, OTP and USIM.	Vulnerable to many types of attacks, including; impersonation and offline password guessing attacks as well as cold-boot attacks. Suffers performance issues and has authentication loopholes.	Mobile Payment Authentication Framework
	[88]	A new concept proposed that claims to overcome relay, DoS and message modification attacks.	No sufficient authentication attack analysis provided using standard validation techniques	Smartphone security service on Clouds
Cloud-Computing	[92]	Security management is handled by network providers	Not verified using standard/automated analysis tools. Keys stored at user-end are vulnerable to impersonation attacks.	Authentication between Cloud and mobile device
	[87]	Employs a multifactor palm-vein and fingerprint authentication mechanism that stored data on a smartcard.	Authentication loophole is found in the storage of sensitive data on smartcards, making it vulnerable to impersonation and password-guessing attack.	Cloud Biometric Authentication using MFA
	[89]	Concept is aimed at relieving mobile computation for performing security and algorithm execution associated with healthcare applications.	The authentication framework is dependent on external provides that do not provide a clear approach in handling external authentications.	CC framework that introduces health-services to mobile devices

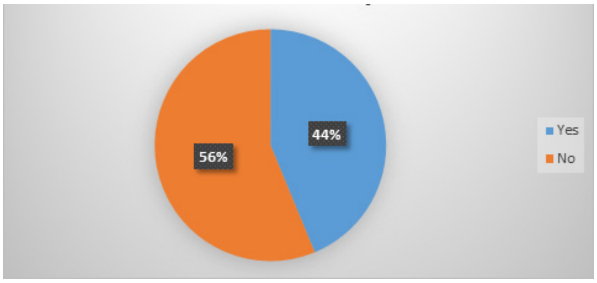

FIGURE 14. Insider attack analysis.

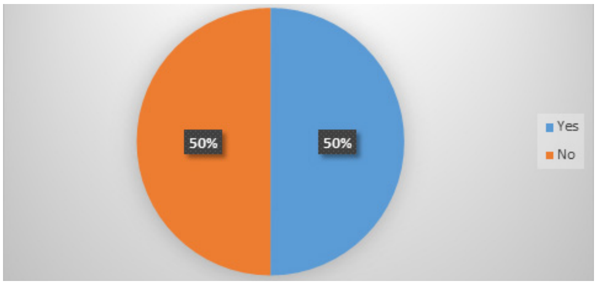

FIGURE 15. Reply attack analysis.

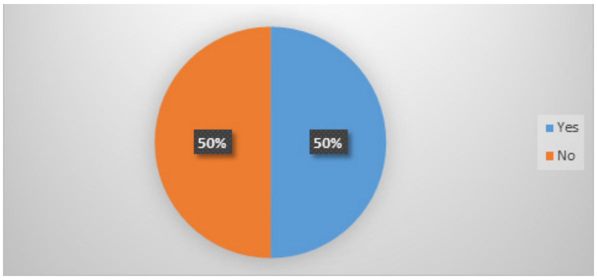

FIGURE 16. Parallel processing attack analysis.

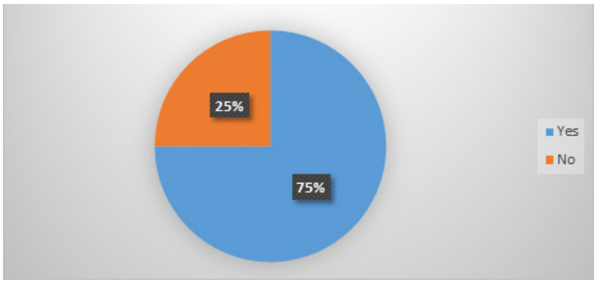

FIGURE 17. Performance analysis.

schemes are vulnerable to online/offline guessing attacks. Figure 14 shows that 44% of authentication schemes are vulnerable to insider attacks. Moreover, Figure 15 and 16 shows that the current authentication schemes are 50% vulnerable to reply and parallel processing attacks. Figure 17 shows that 75% of the current authentication schemes possess performance/computation issues, while Figure 18 shows that 94% of authentication schemes possess implementation issues. Figure 19 illustrates that almost all of the authentication schemes fail to provide sufficient validation and verification of their security claims.

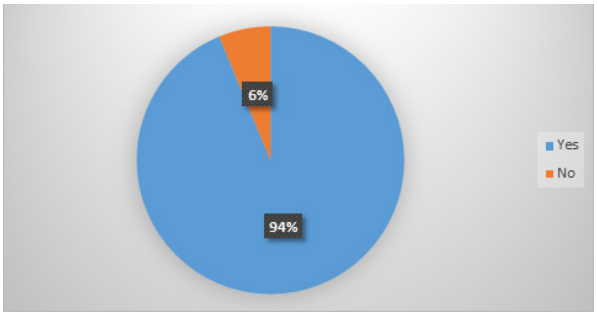

FIGURE 18. Implementation analysis.

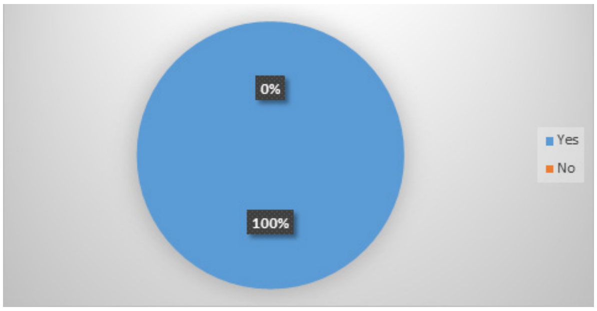

FIGURE 19. Validation analysis.

Table 2 emphasizes on some of the main findings made using a qualitative summary of recent proposals based on key metrics that include: the functionality, practicality and efficiency, and security vulnerability/robustness of each approach.

V. CONCLUSIONS AND FUTURE DIRECTIONS

The use of modern technologies, such as Smartphones, have increased the demand for more secure, reliable and user-friendly authentication systems to facilitate genuine end-users. Existing Smartphone and CC authentication frameworks and protocols are defenseless against a number of authentication and security attacks. This study has performed a detailed review of several authentication frameworks and protocols to outline and address many persistent security issues/flaws and other limitations. The primary objective of this study was to summarize and highlight security vulnerabilities and other alarming issues to discover the current state-of-the-art in the domain. The security vulnerabilities and issues outlined shall assist in enabling the full and complete potential of 3FA authentication frameworks and protocols in Smartphones and CC environments. As a consequence of security flaws and limitations determined in this study, it is clear that additional research work is required in a number of directionsthat consider the following:

- The advent of Smartphone has replaced the use of smartcards from within many domains. However, multifactor and 3FA authentication frameworks and mechanismsare still premature in modern Smartphones like iPhone and Samsung mobiles. Authentication is fragile and can easily be bypassed through several breaches.
- One of the issues was to ignore the re-authentication of authentication factors, while authenticating proceeding authentication factors. For example, after a successful 1FA authentication, the proposed authentication protocolsdo not re-authenticate 1FA, while authenticating 2FA in the next authentication phase.
- Most of the authentication protocols are resource hungry and require a long run of authentication loops. This always causes an unexpected delay during the authentication process.
- Many authentication protocols, whether being proposed for Smartphones or CC, are not developed keeping in mind their relevant implementation scenarios. Some of the authentication frameworks and protocols are not implementable, when considered for practical implementation. It is due to the fact that those solutionsare not cost effective and require extraordinary restructuring.
- In numerous CC authentication frameworks and protocols, complete 3FAs are not implemented due to the limitations of the current state-of-the-art. Dependability of cloud services on third-party resources has made it very delicate to adapt and rely on.
- In addition to the regular authentication phases such as; register, login or authentication, there are other pre-login or pre-authentication phases introduced. The use of unnecessary phases and variables during those phases of authentication has caused various performance issues.

Folllowing a detailed review of a number of Smartphone and CC authentication protocols, the main authentication ambiguities found are now highlighted:

- Storage of sensitive data within smartcards
- Loss or theft of smartcards
- Identity loss during authentication
- Eavesdropping during registration
- Operation interruptions or operational errors
- Resource hungry hardware
- Excessive CPU usage
- Application response time failure
- High memory consumption
- Excess usage of variable and events
- Absence of user security roles
- Service discovery by adversaries
- Client side storage of credentials
- Absence of randomization
- Plain-text storage and processing of information
- Absence of authentication attack analysis
- Vulnerable session variables
- Implementation and validation issues

Due to suchauthentication ambiguities, the entire authentication framework and associatedauthentication protocols are vulnerable to numerous authentication attacks. The following list reveals the vulnerabilities of authentication attacks found in the literature:

- Insider attack
- Impersonation attack
- Reply attack
- Online/Offline password guessing attack
- Parallel processing attack
- Forgery attack
- User/Server anonymity attack
- Man-in-the-Middle attack
- Parallel processing attack
- Impersonation attack
- Denial-of-Service attack
- Shoulder surfing attack

In short, Smartphone and CC technologies were introduced at different times; each technology has its benefits and consequent drawbacks. Likewise, platform dependencies and technology variations had also differed in many ways. In modern days, such technologies and inventions integrate with each other, and therefore require a robust, authentic, light-weight and user friendly authentication framework to deal with existing and forthcoming security threats and liabilities. This paper has identified and highlighted the security pitfalls in the existing Smartphone and CC authentication frameworks and protocols, and has given an analysis of critical security factors in light of those existing studies. The underlined security uncertainties, attacks and future directions in existing Smartphone and CC authentication frameworks have delivered a broader view and awareness of the current state-of-the-art in the domain as well as their practicality for implementation. Finally, this security analysis is expected to open further research opportunities as part of future work in order to address the concerns raised in the domain of Smartphone and CC authentication framework and protocols.

REFERENCES

[1] Z. Siddiqui, A. H. Abdullah, M. K. Khan, and A. S. Alghamdi, "Smart environment as a service: Three factor cloud based user authentication for telecare medical information system," *J. Med. Syst.*, vol. 38, p. 9997, Jan. 2013.

[2] The Statistics Portal. (2014). *Number of Smartphone Users Wordlwide From 2014 to 2020*. [Online]. Available: http://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

[3] Global Privacy Enforcement Network. (2014). *75% of Mobile Apps Want Access to User Data*. [Online]. Available: http://www.futuristgerd.com/wp-content/uploads/2015/03/chartoftheday_2710_App_Privacy_n.jpg

[4] L. Flynn and W. Klieber, "Smartphone security," *IEEE Pervasive Comput.*, vol. 14, no. 4, pp. 16–21, Oct./Dec. 2015.

[5] S. Grzonkowski, A. Mosquera, L. Aouad, and D. Morss, "Smartphone security: An overview of emerging threats," *IEEE Consum. Electron. Mag.*, vol. 3, no. 4, pp. 40–44, Oct. 2014.

[6] A. Ungureanu and C. Costache, "Palm print as a smartphone biometric: Another option for digital privacy and security," *IEEE Consum. Electron. Mag.*, vol. 5, no. 3, pp. 71–78, Jul. 2016.

[7] A. Dardanelli *et al.*, "A security layer for smartphone-to-vehicle communication over bluetooth," *IEEE Embedded Syst. Lett.*, vol. 5, no. 3, pp. 34–37, Sep. 2013.

[8] X. Zhang, J.-P. Seifert, and O. Aciicmez, "Design and implementation of efficient integrity protection for open mobile platforms," *IEEE Trans. Mobile Comput.*, vol. 13, no. 1, pp. 188–201, Jan. 2014.

[9] D. Barrera and P. Van Oorschot, "Secure software installation on smartphones," *IEEE Security Privacy*, vol. 9, no. 3, pp. 42–48, May/Jun. 2011.

[10] S. Gisdakis, V. Manolopoulos, S. Tao, A. Rusu, and P. Papadimitratos, "Secure and privacy-preserving smartphone-based traffic information systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 3, pp. 1428–1438, Jun. 2015.

[11] W. Tan, Y. Fan, A. Ghoneim, M. A. Hossain, and S. Dustdar, "From the service-oriented architecture to the Web API economy," *IEEE Internet Comput.*, vol. 20, no. 4, pp. 64–68, Jul./Aug. 2016.

[12] T. Zhang, S. Zhao, B. Wu, M. Farina, B. Cheng, and J. Chen, "Lightweight SOA-based twin-engine architecture for enterprise systems in fixed and mobile environments," *China Commun.*, vol. 13, no. 9, pp. 183–194, Sep. 2016.

[13] P. C. Hershey, S. Rao, C. B. Silio, and A. Narayan, "System of systems for quality-of-service observation and response in cloud computing environments," *IEEE Syst. J.*, vol. 9, no. 1, pp. 212–222, Mar. 2015.

[14] A. Benharref and M. A. Serhani, "Novel cloud and SOA-based framework for e-health monitoring using wireless biosensors," *IEEE J. Biomed. Health Inform.*, vol. 18, no. 1, pp. 46–55, Jan. 2014.

[15] Q. Duan, Y. Yan, and A. V. Vasilakos, "A Survey on service-oriented network virtualization toward convergence of networking and cloud computing," *IEEE Trans. Netw. Service Manage.*, vol. 9, no. 4, pp. 373–392, Dec. 2012.

[16] S. Berger *et al.*, "Security intelligence for cloud management infrastructures," *IBM J. Res. Develop.*, vol. 60, no. 4, pp. 11-1–11-13, Jul./Aug. 2016.

[17] C. A. Ardagna, M. Conti, M. Leone, and J. Stefa, "An anonymous end-to-end communication protocol for mobile cloud environments," *IEEE Trans. Services Comput.*, vol. 7, no. 3, pp. 373–386, Jul./Sep. 2014.

[18] D. DeFigueiredo, "The case for mobile two-factor authentication," *IEEE Security Privacy*, vol. 9, no. 5, pp. 81–85, Sep./Oct. 2011.

[19] Y. S. Lee, N. H. Kim, H. Lim, H. Jo, and H. J. Lee, "Online banking authentication system using mobile-OTP with QR-code," in *Proc. 5th Int. Conf. Comput. Sci. Converg. Inf. Technol. (ICCIT)*, Seoul, South Korea, Nov./Dec. 2010, pp. 644–648.

[20] K. Fuglerud and O. Dale, "Secure and inclusive authentication with a talking mobile one-time-password client," *IEEE Security Privacy*, vol. 9, no. 2, pp. 27–34, Mar./Apr. 2011.

[21] Z. Siddiqui, A. Abdullah, M. Khan, and A. Alghamdi, "Cryptanalysis and improvement of 'a secure authentication scheme for telecare medical information system' with nonce verification," *J. Peer-to-Peer Netw. Appl.*, vol. 9, no. 5, pp. 841–853, 2016.

[22] O. I. Franko, "Smartphone apps for orthopaedic surgeons," *Clin. Orthopedics Rel. Res.*, vol. 469, no. 7, pp. 2042–2048, 2011.

[23] A. Gutierrez, "Full-system analysis and characterization of interactive smartphone applications," in *Proc. IEEE Int. Symp. Workload Characterization (IISWC)*, Nov. 2011, pp. 81–90.

[24] Z. Siddiqui, A. H. Abdullah, M. K. Khan, and K. Alghathbar, "Analysis of enterprise service buses based on information security, interoperability and high-availability using analytical hierarchy process (AHP) method," *Int. J. Phys. Sci.*, vol. 6, no. 1, pp. 35–42, 2011.

[25] Z. Siddiqui, A. S. Alghamdi, and M. K. Khan, "Node level information security in common information exchange model (CIEM)," *Sci. Int.*, vol. 22, no. 4, pp. 251–258, 2011.

[26] C. K. Agubor, G. A. Chukwudebe, and O. C. Nosiri, "Security challenges to telecommunication networks: An overview of threats and preventive strategies," in *Proc. Int. Conf. Cyberspace (CYBER-Abuja)*, Abuja, Nigeria, Nov. 2015, pp. 124–129.

[27] S. L. Albuquerque and P. R. L. Gondim, "Security in cloud-computing-based mobile health," in *IT Prof.*, vol. 18, no. 3, pp. 37–44, May/Jun. 2016.

[28] R. McKenzie, M. Crompton, and C. Wallis, "Use cases for identity management in E-government," *IEEE Security Privacy*, vol. 6, no. 2, pp. 51–57, Mar. 2008.

[29] J. Kaur and N. Mustafa, "Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME," in *Proc. Int. Conf. Res. Innov. Inf. Syst. (ICRIIS)*, Kuala Lumpur, Malaysia, Nov. 2013, pp. 286–290.

[30] W. Mao, *Modern Cryptography: Theory and Practice*. Upper Saddle River, NJ, USA: Prentice-Hall, 2003.

[31] W. Liu, Q. Xie, S. Wang, and B. Hu, "An improved authenticated key agreement protocol for telecare medicine information system," *SpringerPlus*, vol. 5, p. 555, Dec. 2016.

[32] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.* vol. 17, no. 4, pp. 960–969, Apr. 2016.

[33] C. Boyd and A. Mathuria, "Password-based protocols," in *Protocols for Authentication and Key Establishment*. Berlin, Germany: Springer, 2003, pp. 247–288.

[34] P. Salmela and J. Melén, "Host identity protocol proxy," in *E-business and Telecommunication Networks*, J. Filipe, H. Coelhas, and M. Saramago, Eds. Berlin, Germany: Springer, 2007, pp. 126–138.

[35] E.-J. Yoon, W.-S. Lee, and K.-Y. Yoo, "Secure PAP-based RADIUS protocol in wireless networks," in *Advanced Intelligent Computing Theories and Applications. With Aspects of Contemporary Intelligent Computing Techniques*, D.-S. Huang, L. Heutte, and M. Loog, Ed. Berlin, Germany: Springer, 2007, pp. 689–694.

[36] A. Leicher, A. U. Schmidt, and Y. Shah, "Smart OpenID: A smart card based OpenID protocol," in *Information Security and Privacy Research*, D. Gritzalis, S. Furnell, and M. Theoharidou, Eds. Berlin, Germany: Springer, 2012, pp. 75–86.

[37] T.-H. Chen, H.-L. Yeh, and W.-K. Shih, "An advanced ECC dynamic ID-based remote mutual authentication scheme for cloud computing," in *Proc. 5th FTRA Int. Conf. Multimedia Ubiquitous Eng. (MUE)*, Jun. 2011, pp. 155–159.

[38] S. Kumari and M. K. Khan, "More secure smart card-based remote user password authentication scheme with user anonymity," *Secur. Commun. Netw.*, vol. 7, no. 11, pp. 2039–2053, 2014.

[39] S. Kumari and M. K. Khan, "Cryptanalysis and improvement of 'a robust smart-card-based remote user password authentication scheme,'" *Int. J. Commun. Syst.*, vol. 27, no. 12, pp. 3939–3955, 2013.

[40] FFIEC. (Mar. 1979). *Federal Financial Institutions Examination Council*. [Online]. Available: https://www.ffiec.gov/

[41] PCI DSS. (Dec. 2004). *Payment Card Industry Data Security Standards*. [Online]. Available: https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

[42] B. Coskun and C. Herley, "Can 'something you know' be saved?" in *Information Security*, T.-C. Wu, C.-L. Lei, V. Rijmen, and D.-T. Lee, Ed. Berlin, Germany: Springer, 2008, pp. 421–440.

[43] B. Lakshmiraghavan, "Two-factor authentication," in *Pro ASP.NET Web API Security*. New York, NY, USA: Apress, 2013, pp. 319–343.

[44] J. Fierrez *et al.*, "BiosecurID: A multimodal biometric database," *Pattern Anal. Appl.*, vol. 13, no. 2, pp. 235–246, 2010.

[45] A. A. Al-Qahtani, "Formal approaches for specifying, enforcing, and verifying security policies," Ph.D. dissertation, Univ. Idaho, Moscow, ID, USA, 2003, p. 177.

[46] A. Alghamdi, M. Nasir, I. Ahmad, and K. A. Nafjan, "An interoperability study of ESB for C4I systems," in *Proc. Int. Symp. Inf. Technol. (ITSim)*, Jun. 2010, pp. 733–738.

[47] C. Doukas, T. Pliakas, and I. Maglogiannis, "Mobile healthcare information management utilizing cloud computing and Android OS," in *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Aug./Sep. 2010, pp. 1037–1040.

[48] X. Fan and G. Gong, "Securing NFC with elliptic curve cryptography—Challenges and solutions," in *Proc. Radio Freq. Identificat. Syst. Secur. (RFIDsec) Asia Workshop*, vol. 97, 2013, pp. 97–106

[49] Z.-Y. Wu, Y.-C. Lee, F. Lai, H.-C. Lee, and Y. Chung, "A secure authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 36, no. 3, pp. 1529–1535, 2012.

[50] Z. Zhu, "An efficient authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 36, no. 6, pp. 3833–3838, 2012.

[51] X. Yan, W. Li, P. Li, J. Wang, X. Hao, and P. Gong, "A secure biometrics-based authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 37, p. 9972, Oct. 2013.

[52] Q. Jiang, J. Ma, X. Lu, and Y. Tian, "Robust chaotic map-based authentication and key agreement scheme with strong anonymity for telecare medicine information systems," *J. Med. Syst.*, vol. 38, p. 12, Feb. 2014.

[53] J. Wei, X. Hu, and W. Liu, "An improved authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 36, no. 6, pp. 3597–3604, 2012.

[54] H.-M. Chen, J.-W. Lo, and C.-K. Yeh, "An efficient and secure dynamic ID-based authentication scheme for telecare medical information systems," *J. Med. Syst.*, vol. 36, no. 6, pp. 3907–3915, 2012.

[55] F. T. B. Muhaya, "Cryptanalysis and security enhancement of Zhu's authentication scheme for telecare medicine information system," *Secur. Commun. Netw.*, vol. 8, no. 2, pp. 149–158, 2014.

[56] P. Salmela and J. Melén, "Host identity protocol proxy," in *E-business and Telecommunication Networks*, J. Filipe, H. Coelhas, and M. Saramago, Eds. Berlin, Germany: Springer, 2007, pp. 126–138.

[57] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal DoS attack scheduling in wireless networked control system," *IEEE Trans. Control Syst. Technol.* vol. 24, no. 3, pp. 843–852, May 2016.

[58] M. Sabt and J. Traoré, "Breaking into the keystore: A practical forgery attack against Android keystore," in *Proc. Eur. Symp. Res. Comput. Secur.*, Heraklion, Greece. Berlin, Germany: Springer, Sep. 2016, pp. 531–548.

[59] H. Abdalla, X. Hu, A. Wahaballa, P. Avornyo, and Q. Zhiguang, "Anonymous pairing-free and certificateless key exchange protocol for DRM system," *Int. J. Netw. Secur.*, vol. 18, no. 2, pp. 235–243, 2016.

[60] I. Ahmad, A. B. Abdullah, and A. S. Alghamdi, "Evaluating neural network intrusion detection approaches using analytic hierarchy process," in *Proc. Int. Symp. Inf. Technol. (ITSim)*, Jun. 2010, pp. 885–890.

[61] T. Cao and J. Zhai, "Improved dynamic ID-based authentication scheme for telecare medical information systems," *J. Med. Syst.*, vol. 37, p. 9912, Apr. 2013.

[62] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proc. R. Soc. Lond. A, Math. Phys. Sci.*, vol. 426, no. 1871, pp. 233–271, 1989.

[63] P. Syverson and I. Cervesato, "The logic of authentication protocols," in *Foundations of Security Analysis and Design*, R. Focardi and R. Gorrieri, Eds. Berlin, Germany: Springer, 2001, pp. 63–137.

[64] R. Küsters and T. Truderung, "Using ProVerif to analyze protocols with Diffie–Hellman exponentiation," in *Proc. 22nd IEEE Comput. Secur. Found. Symp. (CSF)*, 2009, pp. 157–171.

[65] C. J. F. Cremers, *Scyther: Semantics and Verification of Security Protocols*. Eindhoven, The Netherlands: Technische Univ. Eindhoven, 2006.

[66] D. Mishra, S. Mukhopadhyay, A. Chaturvedi, S. Kumari, and M. K. Khan, "Cryptanalysis and improvement of Yan *et al.*'s biometric-based authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 38, p. 24, Jun. 2014.

[67] A. Awasthi and K. Srivastava, "A biometric authentication scheme for telecare medicine information systems with nonce," *J. Med. Syst.*, vol. 37, p. 9964, Oct. 2013.

[68] A. K. Das and A. Goswami, "An enhanced biometric authentication scheme for telecare medicine information systems with nonce using chaotic hash function," *J. Med. Syst.*, vol. 38, p. 27, Jun. 2014.

[69] D. Mishra, S. Mukhopadhyay, S. Kumari, M. K. Khan, and A. Chaturvedi, "Security enhancement of a biometric based authentication scheme for telecare medicine information systems with nonce," *J. Med. Syst.*, vol. 38, p. 41, May 2014.

[70] C. J. F. Cremers, "The scyther tool: Verification, falsification, and analysis of security protocols," in *Proc. Int. Conf. Comput. Aided Verification*. Berlin, Germany: Springer, Jul. 2008, pp. 414–418.

[71] O. Tayan, "Concepts and tools for protecting sensitive data in the IT industry: A review of trends, challenges and mechanisms for data-protection," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 2, pp. 46–52, Mar. 2017.

[72] A. Boldyreva and V. Kumar, "Provable-security analysis of authenticated encryption in Kerberos," *IET Inf. Secur.*, vol. 5, no. 4, pp. 207–219, 2011.

[73] J. P. Degabriele, K. Paterson, and G. Watson, "Provable security in the real world," *IEEE Security Privacy*, vol. 9, no. 3, pp. 33–41, May/Jun. 2011.

[74] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1900–1910, May 2018.

[75] S. Goldwasser and S. Micali, "Probabilistic encryption," *J. Comput. Syst. Sci.*, vol. 28, no. 2, pp. 270–299, 1984.

[76] M. Bellare and C. Namprempre, "Authenticated encryption: Relations among notions and analysis of the generic composition paradigm," in *Advances in Cryptology ASIACRYPT* (Lecture Notes in Computer Science). Berlin, Germany: Springer, Dec. 2000, pp. 531–545.

[77] S. Madhusudhanan and S. Mallissery, "Provable security analysis of complex or smart computer systems in the smart grid," in *Proc. IEEE Int. Conf. Smart Grid Smart Cities*, Jul. 2017, pp. 210–214.

[78] C. Shen, Y. Zhang, X. Guan, and R. A. Maxion, "Performance analysis of touch-interaction behavior for active smartphone authentication," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 3, pp. 498–513, Mar. 2016.

[79] A. Alzubaidi and J. Kalita, "Authentication of smartphone users using behavioral biometrics," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1998–2026, 3rd Quart., 2016.

[80] P. Gasti, J. Šeděnka, Q. Yang, G. Zhou, and K. S. Balagani, "Secure, fast, and energy-efficient outsourced authentication for smartphones," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2556–2571, Nov. 2016.

[81] J.-L. Tsai and N.-W. Lo, "A privacy-aware authentication scheme for distributed mobile cloud computing services," *IEEE Syst. J.*, vol. 9, no. 3, pp. 805–815, Sep. 2015.

[82] B. En-Nasry and M. D. E. C. El Kettani, "Towards an open framework for mobile digital identity management through strong authentication methods," in *Proc. FTRA Int. Conf. Secure Trust Comput., Data Manage., Appl.*, Loutraki, Greece. Berlin, Germany: Springer, Jun. 2011, pp. 56–63.

[83] J.-Y. Hu, C.-C. Sueng, W.-H. Liao, and C. C. Ho, "Android-based mobile payment service protected by 3-factor authentication and virtual private ad hoc networking," in *Proc. Comput., Commun. Appl. Conf. (ComComAp)*, Jan. 2012, pp. 111–116.

[84] M. Günther and B. Borchert, "Online banking with NFC-enabled bank card and NFC-enabled smartphone," in *Information Security Theory and Practice. Security of Mobile and Cyber-Physical Systems*, L. Cavallaro and D. Gollmann, Eds. Berlin, Germany: Springer, 2013, pp. 66–81.

[85] H. Wang, S. Wu, M. Chen, and W. Wang, "Security protection between users and the mobile media cloud," *IEEE Commun. Mag.*, vol. 52, no. 3, pp. 73–79, Mar. 2014.

[86] I. Al Rassan and H. AlShaher, "Securing mobile cloud computing using biometric authentication (SMCBA)," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Mar. 2014, pp. 157–161.

[87] S. Ziyad and A. Kannammal, "A multifactor biometric authentication for the cloud," in *Computational Intelligence, Cyber Security and Computational Models*. Berlin, Germany: Springer, 2014, pp. 395–403.

[88] P. Urien and S. Piramuthu, "Securing NFC mobile services with cloud of secure elements (CoSE)," in *Proc. Int. Conf. Mobile Comput., Appl., Services*, Paris, France. Berlin, Germany: Springer, Nov. 2013, pp. 322–331.

[89] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," *Wireless Commun. Mobile Comput.*, vol. 13, no. 18, pp. 1587–1611, Dec. 2013.

[90] F. Omri, S. Foufou, R. Hamila, and M. Jarraya, "Cloud-based mobile system for biometrics authentication," in *Proc. 13th Int. Conf. ITS Telecommun. (ITST)*, Nov. 2013, pp. 325–330.

[91] A. N. Khan, M. L. M. Kiah, S. A. Madani, A. ur Rehman Khan, and M. Ali, "Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing," *J. Supercomput.*, vol. 66, no. 3, pp. 1687–1706, 2013.

[92] M. Al-Hasan, K. Deb, and M. O. Rahman, "User-authentication approach for data security between smartphone and cloud," in *Proc. 8th Int. Forum Strategic Technol. (IFOST)*, Jun./Jul. 2013, pp. 2–6.

[93] S. S. Sundar, S. Bellur, and H. Jia, "Motivational technologies: A theoretical framework for designing preventive health applications," in *Persuasive Technology. Design for Health and Safety*, M. Bang and E. Ragnemalm, Eds. Berlin, Germany: Springer, 2012, pp. 112–122.

[94] H. Debiao, C. Jianhua, and Z. Rui, "A more secure authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 36, no. 3, pp. 1989–1995, 2012.

[95] T.-F. Lee and C.-M. Liu, "A secure smart-card based authentication and key agreement scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 37, no. 3, pp. 1–8, 2013.

[96] T. Cao and J. Zhai, "Improved dynamic id-based authentication scheme for telecare medical information systems," *J. Med. Syst.*, vol. 37, p. 9912, Apr. 2013.

[97] Q. Xie, J. Zhang, and N. Dong, "Robust anonymous authentication scheme for telecare medical information systems," *J. Med. Syst.*, vol. 37, p. 9911, Apr. 2013.

[98] X. Hao, J. Wang, Q. Yang, X. Yan, and P. Li, "A chaotic map-based authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 37, p. 9919, Apr. 2013.

[99] T.-H. Lin and T.-F. Lee, "Secure verifier-based three-party authentication schemes without server public keys for data exchange in telecare medicine information systems," *J. Med. Syst.*, vol. 38, p. 30, May 2014.

[100] L. Gkatzikis and I. Koutsopoulos, "Migrate or not? exploiting dynamic task migration in mobile cloud computing systems," *IEEE Wireless Commun.*, vol. 20, no. 3, pp. 24–32, Jun. 2013.

[101] T. Munkelt and S. Völker, "ERP systems: Aspects of selection, implementation and sustainable operations," *Int. J. Inf. Syst. Project Manage.*, vol. 1, no. 2, pp. 25–39, 2013.

[102] H.-C. Chen and E. Prater, "Information system costs of utilizing electronic product codes in achieving global data synchronization within the pharmaceutical supply chain network," *Int. J. Inf. Syst. Supply Chain Manage.*, vol. 6, no. 1, pp. 62–76, 2013.

[103] A. Gani, G. M. Nayeem, M. Shiraz, M. Sookhak, M. Whaiduzzaman, and S. Khan, "A review on interworking and mobility techniques for seamless connectivity in mobile cloud computing," *J. Netw. Comput. Appl.*, vol. 43, pp. 84–102, Aug. 2014.

[104] S. Iqbal *et al.*, "On cloud security attacks: A taxonomy and intrusion detection and prevention as a service," *J. Netw. Comput. Appl.*, vol. 74, pp. 98–120, Oct. 2016.

[105] S. Khan *et al.*, "Cloud log forensics: Foundations, state of the art, and future directions," *ACM Comput. Surv.*, vol. 49, no. 1, 2016, Art. no. 7.

[106] S. Khan *et al.*, "Towards an applicability of current network forensics for cloud networks: A SWOT analysis," *IEEE Access*, vol. 4, pp. 9800–9820, 2016.

ZEESHAN SIDDIQUI is currently an Assistant Professor with the Modern College of Business and Sciences. He is specialized in remote user digital authentication and security, command and control systems (C2/C3/C4I), enterprise architectures middleware, and cloud computing remote user authentication. He is a member of the American Association of Science and Technology and the IBM Academic Initiative. He is also a Reviewer of IJEIS, IJSEKE, IJSCN, IJCEN, and other ISI Journals. He is an editor of several international journals.

OMAR TAYAN (S'03–M'10) received the B.Eng. and Ph.D. degrees in computer networks from the University of Strathclyde, Glasgow, U.K. He was a Consultant with the Strategic and Advanced Research and Technology Innovation Unit, Taibah University, Saudi Arabia. He is currently an Associate Professor with the NOOR Research Center, College of Computer Science and Engineering, Taibah University, where he is also one of the Founding Members of the NOOR Research Center. He has successfully completed about 10 research and development projects as a principle investigator and a co-investigator in projects funded by the King AbdulAziz City of Science and Technology, Ministry of Higher Education, and the Deanship of Research, Taibah University. He currently has about 50 journals, conference papers, technical reports, and invited talks to his credit, as well as a book publication in computer networks. His research interests include information security, E-Learning and multimedia technologies, Quranic computing, image processing, modeling and simulation, computer networks and networks-on-chip, and wireless sensor networks for intelligent transportation systems, including Hajj transportation systems and crowd management.

MUHAMMAD KHURRAM KHAN is one of the Founding Members of the Center of Excellence in Information Assurance (CoEIA) and has served as the Manager of research and development from 2009 to 2012. He developed and successfully managed the research program of CoEIA, which transformed the center as one of the best centers of research excellence in Saudi Arabia as well as in the region. He is currently a Full Professor with CoEIA, King Saud University, Saudi Arabia.

Mr. Khurram Khan has been the Editor-in-Chief of a well-esteemed ISI-indexed international journal *Telecommunication Systems* (Springer-Verlag) since 1993 with an impact factor of 1.542 (JCR 2016). He is a Founding Editor of the *Bahria University Journal of Information and Communication Technology*. Furthermore, he is also a full-time Editor/Associate Editor of several ISI-indexed international journals/magazines, including the IEEE Communications Surveys and Tutorials, *IEEE Communications Magazine*, the *Journal of Network and Computer Applications* (Elsevier), the IEEE Transactions on Consumer Electronics, the IEEE Access, *Security and Communication Networks*, *IEEE Consumer Electronics Magazine*, the *Journal of Medical Systems* (Springer), *PLOS One*, *Computers & Electrical Engineering* (Elsevier), *IET Wireless Sensor Systems*, *Electronic Commerce Research* (Springer), the *Journal of Computing and Informatics*, the *Journal of Information Hiding and Multimedia Signal Processing*, the *International Journal of Biometrics* (Inderscience), and so on.

He is also an Adjunct Professor with the Fujian University of Technology, China, and an Honorary Professor with IIIRC, Shenzhen Graduate School, Harbin Institute of Technology, China. He received the Outstanding Leadership Award from the IEEE International Conference on Networks and Systems Security, Australia, in 2009. He has been included in the Marquis Who's Who in the World 2010 edition. Besides, he has received certificate of appreciation for outstanding contributions in Biometrics & Information Security Research at the AIT international Conference, Japan, in 2010.

He received the Gold Medal for the Best Invention and Innovation Award at the 10th Malaysian Technology Expo 2011, Malaysia. Moreover, his invention recently received the Bronze Medal at the 41st International Exhibition of Inventions, Geneva, Switzerland, in 2013. In addition, he received the Best Paper Award from the *Journal of Network and Computer Applications* (Elsevier) in 2015.

He has played a leading role in developing the B.S. Cybersecurity Degree Program and the Higher Diploma in cybersecurity with King Saud University. He has secured several national and international research grants in the domain of information security. He has edited seven books/proceedings published by Springer-Verlag and the IEEE. He has published over 300 research papers in the journals and conferences of international repute. In addition, he is an inventor of 10 U.S./PCT patents. His research areas of interest are cybersecurity, digital authentication, biometrics, multimedia security, and technological innovation management. He is a fellow of IET (U.K.), BCS (U.K.), FTRA (South Korea), and a member of the IEEE Technical Committee on Security and Privacy and the IEEE Cybersecurity Community. He was a recipient of the King Saud University Award for Scientific Excellence (Research Productivity) in 2015, and the King Saud University Award for Scientific Excellence (Inventions, Innovations, and Technology Licensing) in 2016.