I.J. Information Technology and Computer Science, **2015, 05, 67-76**
Published Online April 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2015.05.10

Secure Hajj Permission Based on Identifiable Pilgrim's Information

Ebtehal Alsaggaf, Omar Batarfi, Nahla Aljojo
Faculty of Computing and Information Technology, King Abdul Aziz University, P.O. Box, 80200, Jeddah, 21589, KSA
Email: {eaalsaggaf, obatarf, naljojo}@kau.edu.sa

Carl Adams
School of Computing , University of Portsmouth, Portsmouth, UK, Buckingham Building, Lion Terrace, Portsmouth PO1 3HE
Email: carl.adams@port.ac.uk

Abstract— Event management of large international events is attracting interest from researchers, not least due to the potential use of technology to provide support throughout the different stages of the event. Some events, such as major sports or religious events, can involve millions of people from different countries, and require active management to control access (e.g. many popular events can be oversubscribed) and to reduce risks for the participants, local communities and environment. This paper explores the context of a large event - the Hajj pilgrims in Saudi Arabia - which involves up to three million pilgrims, many of whom are international. The paper presents a novel identification system - the Identification Wristband Hajj Permission (IWHP) - which uses encryption technologies and biometric attributes to identify pilgrims, whilst remaining sensitive to the context of the Hajj. The suggested solution has many attributes of relevance that could support its use in other large-crowd events.

Index Terms— Biometric, Cryptosystem, Hajj permission, IWPH, RFID Wristband

I. Introduction

Event management of large international events is attracting interest from researchers, not least due to the potential use of technological support in managing such events. Goldblatt [1] argues that humans have an intrinsic need to join together for rituals and ceremonies, and with the move towards a global, connected world, these events are likely to get bigger and involve more people from different nations. Some events, such as major sports or religious activities, can involve hundreds of thousands or millions of participants. Horne and Manzenreiter [2] highlight the global phenomenon of mega sporting events, such as the Olympics and the FIFA World Cup. They identify the often complex organisational, resource and financial aspects of such events requiring active management to ensure that the events progress successfully and safely. These mega events have a global reach; the use of mass communication technologies make the event newsworthy and attract large amounts of money in the form of sponsorship, as well as requiring significant changes to local infrastructure and resources to cope. The impact on host cities, regions and nations of such large events can be considerable, as the hosts have to accommodate for masses over a relatively short period of time, all requiring a range of facilities such as food, accommodation, transport and even healthcare. There are tradeoffs with hosting such events: on the one hand, these events bring positive long term sociological, economic, and political benefits for the host; on the other hand, these events bring major disruption and require considerable resources and investments in aspects such as extra infrastructure and active management [3, 4]. The level of funds required to host such mega events can be huge, as can be seen from the hosting of the Olympics; the 2008 Beijing Games is estimated to have cost about $40 billion, whilst Sochi 2014 Winter Games cost $50 billion [5].

There are limits to resources in any hosting environment (accommodation, transport, infrastructures). Many popular events can be oversubscribed, often significantly, which requires some active management to ensure the fair allocation of places for potential participants [1-3, 6]. Once allocation of places has been completed, the requirements of attending visitors need to be monitored, managed and policed to ensure only valid participants attend the event. The allocation and control of visitors at a mass event is a non-trivial activity and increases in complexity as the scale of the event increases. The accumulation of a mass of visitors raises issues over security and risks for the participants, as well as the local communities and environment [3, 7]. Memish et al [8] identify the potential public health issues of mass gatherings, highlighting the need to possess the ability to contain potential infectious diseases, and given the likely international participants at such events, to be able to reinforce global health security. Yamin and Ades [9] identify some significant challenges such as the potential spread of communicable diseases; the potential for crowd problems, such as stampedes of masses of people in confined spaces; and a more general set of ongoing security issues. Similarly, Bowdin et al [7] argue there are many areas of risk throughout the whole process of organising and hosting large events, and suggests a nine-step approach to risk management of such events. Tarlow [10] suggests a similar set of activities for managing the risks in major events and for providing security for the participants. Managing and supporting events with very large crowds is complex, involving many issues and many areas of risk; as the events increase in size, so too does the level of risk and the need to actively manage all stages of the event - initial planning, promoting, running and post-event activity.

Whilst sport is considered the key area of mega event management, a further area is that of religious festivals and pilgrimages. An example of this is the Maha Kumbh Mela, which takes place once every 12 years in India and attracts huge numbers of pilgrims: "January 14th [2013] sees the start of the Maha Kumbh Mela - a mass Hindu pilgrimage - the biggest religious event in the world. Nothing else compares to the scale of this ancient Hindu Festival. The Mela happens every 12 years and, in 2001, more than 40 million people attended on the main bathing day, breaking the world record for the largest human gathering in one place" [11]. A more frequent mass pilgrimage is the Hajj in Saudi Arabia, which can involve up to three million pilgrims and has a more international mix of visitors [12]. Eid [13] argues that the Hajj (Pilgrimage) is a unique and universal Islamic event, taking place annually, in Makkah, Saudi Arabia. Hajj consists of performing specific prayers at sacred places and is obligatory as one of the five pillars of Islam. Thus there is an expectation that all Muslims, if they have the capacity, should attend Hajj at least once in their life. The focus of this paper then is on developing support technologies for religious mega events such as the Hajj pilgrimage. For the hosts of such mega events (sport, cultural or religious events), coordinating these events is a complex and responsibility-laden activity, as they have a duty of care for the visitors attending and for the local community and environment in which the event occurs [2, 14]. Silvers et al [14] argue that event management is becoming a sub multi-discipline in its own right, developing its own body of knowledge, regulation, qualifications and best practice. As a result, the application of technology is becoming key to all the stages of managing these massive, complex and increasingly international events.

Eid [13] investigated the quality of the Hajj experience from the pilgrims' perspective. This study captured pilgrim representation from five different countries, emphasizing the international nature of the Hajj, and found that for these pilgrims reliability, responsiveness, assurance, and empathy were important for a safe experience. Achieving this for three million visitors annually is a massive undertaking, requiring active management, and of course technological support. Henderson [15] argues that there is a close relationship between religious pilgrim events and tourism as they share a similar set of challenges, such as providing travel and wider infrastructure, and maintaining the variety of visitor attractions. Globally, an increase in wealth and ability to travel has consequently led to an increase in the number of people wanting to make a Hajj pilgrimage. Henderson [15] also considers the Hajj, and the practical changes to allow for the Saudi Arabia government's pursuit of a policy to expand the numbers of pilgrims which can be accommodated. Jafari and Scott [16] argue there is a growing number of Muslim travelers to Hajj and other pilgrimage events, and that the need for increased accommodation is of practical importance for the tourism industry. There is a need to understand the requirements of the mass pilgrimage and to develop solutions that are sensitive to the context of the pilgrims. For instance, in the context of Islam, identification by face, or face recognition technologies, would cause embarrassment to the pilgrims during inspection.

Memish et al [8] identify a need to actively manage and monitor the enrolment of individuals attending the Hajj as a means to ensuring the wellbeing of all pilgrims and to contain any potential infectious diseases – not just for the pilgrims, but also to ensure global health security. Bahurmoz [3] suggests a strategic model of safety during the Hajj pilgrimage, using Analytic Network Process techniques to provide a holistic view to structure the complex set of challenges involved in managing the Hajj context. Being sensitive to the context of the Hajj pilgrimage involves technological support that is nonintrusive. Mantoro et al [17] propose a framework for tracking Hajj pilgrims based on mobile phone environments, and have developed a prototype called the Hajj Locator. Yamin [18] and Yamin and Ades [9] suggest using radio-frequency identification (RFID) technologies to help track and monitor participants at massive events such as Hajj and Kumbh. They suggest a management and technological framework for applying RFID-based support for large and dense crowds of visitors to events. RFID solutions have previously been used widely to track and monitor participants at large events, such as marathons. The suitability of this approach arises from the fact that IT is often seen as cheap, small, unobtrusive and reliable technology that individuals can carry in one form or another.

This paper builds on the need to be sensitive to the context of the Hajj environment, such as personal modesty, and a need for a convenient and effective way of identifying people without permanently marking them that is robust and scalable. The suggested solution also builds on the application of RFID technologies as per [9, 18] in the form of wristbands, but extends the application to include more robust identification capabilities using biometric information embedded within the devices. The resultant system is referred to as the Identification Wristband Hajj Permission (IWHP), and although it is aimed primarily at the Hajj, it has attributes that can be applied more widely at other events that require robust identification of participants. It is also relatively cheap and is scalable in terms of accommodating for very large numbers of participants. The IWHP solution suggests three digital signature algorithms within a proposed architecture that provides improvements to the traditional means of providing identification and verification of pilgrims. The paper will then describe the development of the proposed IWHP and discuss its application. The paper will be structured as follows: the introduction will provide more background on Hajj, and Section 2and 3 will present an overview of the three technologies and further the literature review. The system architecture will be presented through a focus on the three algorithms mentioned earlier. Section VI provides the analysis and results of the system. Sections VII&V conclude this paper.

II. Hajj and RFID Technologies

Hajj is the fifth pillar of the Islam, an annual meeting of the Islamic world for all Muslims from different parts of the world. Whilst the pilgrims are generally international, many are from within Saudi Arabia or other Gulf countries. There is a growing but limited capacity at the holy sites, a capacity that has to be distributed to the various internal Hajj missions. In order to facilitate the needs of Hajj and the safety of pilgrims, the Ministry of Hajj issues permits to serve and provide comfort for the pilgrims and to determine the number of pilgrims. There are also challenges in the issue of permits, such as coping with increasing numbers of pilgrims, and in dealing with forgery of Hajj permissions by fake expedition's or the selling of Hajj permissions to people who have been barred from attending [19].

Reducing the risk of forgery, theft, or abuse of identification credentials requires more robust authentication, such as that afforded by the use of encryption, and digital signatures. A more robust authentication approach is also seen as a requirement to secure borders, protect and allocate public assets and resources and to boost overall citizen satisfaction [20].

Today, the RFID wristband is often seen as the cornerstone of efficient and secure access control and payment for events, as well as providing a convenient and effective way of identifying people [21-23]. Furthermore, the proposed IWHP approach introduces Biometrics in the identification of the individual, which can provide increased authentication capability of individuals, based on identity attributes that cannot be stolen or forgotten and are very difficult to forge [24, 25].

Many ideas and techniques have been proposed by researchers for transportation and crowd management. The Hajj workshop [26] in particularly discussed a number of urgent topics in the field of transportation and crowd management. Some of these techniques were implemented and proved their success, while others were either not implemented, or have been implemented with limited success .Much research exists that discusses using PKI/smart cards [27-29]. The use of PKI/smart cards can increase the levels of security at events, as they provide a sole application on which digital signatures and encrypted data can be developed and stored. Federated Identity proffered the use of a smart card similar to those used in Personal Identity Verification (PIV), which utilize PKI, digital signatures, biometric data, printed information and face-recognition through a photo. A tamper-proof form of security, in the form of these PKI/smart cards, satisfies the criteria of the security specifications stipulated.

The system used in this study is somewhat similar to the Federated Identity system, as it uses an RFID wristband, fingerprints and the digital signature techniques of PKI. RFID technology's radio link function is not much different from that of many types of non-contact smart cards, in that it communicates with a Bluetooth local network and may issue or receive commands or data, including voice data. A principle advantage of a wristband is that it is ultimately removable. In 2008, Mohamed Mohandes presented a solution based on RFID technology to help the Hajj authorities in the identification of pilgrims.

This study will improve that solution by adding PKI Authentication and using biometric technology to automatically verify the identity of pilgrims. In 2008, Taekyoung Kwon and Hyeonjoon Moon presented several challenges in border control applications. The main concerns of this paper include the first three challenges, as well as privacy infringement issues. The several challenges in border control applications are:

- The costs incurred in processing biometric information;
- The costs incurred in issuing smart-card ready passports globally;
- Biometrics are generally only suitable in small-scale applications;
- The reluctance of bearers to supply biometric information to officers as a result of personal preference.

These challenges will be resolved through the use of wristbands, fingerprints and a small-scale database across Saudi Arabia. In 2009, The Republic of Indonesia applied multi-biometric technology to its Integrated Biometric Passport Issuance System. This method solved the issue of the potential to duplicate passport issuance in a simple and low cost manner. This study will use the idea of this passport enrollment system to develop a more effective and secure system by adding PKI Authentication and RFID technology. In this paper, the proposed system of issuing a pilgrimage consists of three algorithms: key generation, signing, and signature verifying algorithms. They rely on the biometric feature of a match and hash logic match, which combines the advantage of mathematical equations of RSA algorithm and asymmetric key cryptography [30]. Thus, the Hajj permissions will be afforded a high level of PKI authentication and provide features that increase accuracy and usability. Hajj permissions will combine biometric identification and the RFID Wristband to verify the authentication of pilgrims and to limit the number of pilgrims in holy places (See sections A, B, C, D, &E). If these systems are applied to Hajj, the event will be provided with authentication, access control, and valid systems.

A. Public Key Infrastructure (PKI) Technology

A public key infrastructure is a key management system that certifies individuals, programs and systems and proffers public-key and encryption services for network applications, through digital signatures and other keys. There are six key stages in the PKI system: certification (CA), registration (RA), certificate pools, key backup and storage, retrieval systems and the application interface. PKI is afforded as a means of ensuring confidentiality when transmitting data and verifying any occurring transactions. PKI is considered a suitable means of transmitting and storing data in a confidential manner, having been heavily researched and development. Despite this, some limitations exist around PKI. The use of an asymmetric encryption algorithm or hash-algorithm has led to the cracking of public key's becoming almost impossible; however, the dependence on an overly-centralized system of storage has led to all data likely to be stolen found in one location [30, 31]. Alongside this, the PKI authentication system can become obsolete if private keys are forged or lost [32]. As such, PKI necessitates public key cryptography. Public key cryptography uses mathematical algorithms and methods to translate comprehensible plaintext to indecipherable cipher text. Applications of cryptography involve:

- Data encryption for confidentiality
- Digital signatures to provide non-repudiation (accountability)
- Verification of data integrity
- Certificates for authenticating people, applications and services, and for access control (authorization) [33].

Our study will focus on asymmetric cryptography, hash- function and mathematics to describe the authentication that confirms an identity credential belongs to the individual present.

B. Biometric Technologies

Through the processing of a unique physiological characteristic, biometric technologies are used to confirm the identity of an individual. As a result, biometrics is considered a secure and convenient means of authentication, as it is relatively difficult to steal or forge. A fingerprint, iris print, or eye blood vessel pattern can be used to determine the identity of an individual. However, some biometric devices are considered intrusive and insensitive. As such, the system proposed here will use fingerprint technology as it is relatively unobtrusive [25, 35].

a. The Biometric System

Both enrollment and verification are required in the biometric system. Enrollment involves ascertaining an individual's biometric image, through for example a fingerprint, in order to create a unique biometric user template. This biometric template is garnered for use in the verification stage, and is held on a database or machine readable card until this time. The enrollment process can be seen in "Fig. 1".

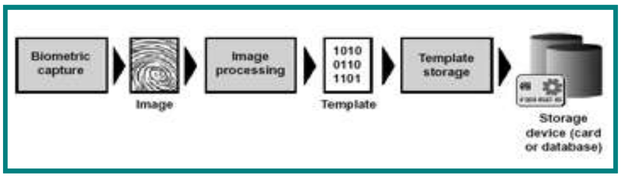

Fig. 1. Example Enrollment Process [24]

The identify verification stage recaptures the biometric image of the user to obtain the unique user template, which is considered 'live.' A comparison is then undertaken to ensure that the new biometric template corresponds to the previous template captured in the enrollment process. The comparison uses a numerical scale which highlights the duplication percentage between the two templates. A minimal error threshold is provided within the system to ensure the security of the system is upheld see "Fig. 2".

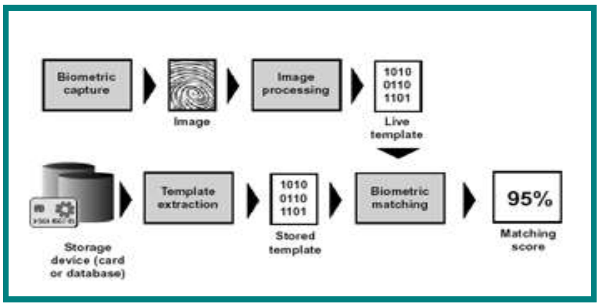

Fig. 2. Example Verification Process [24]

Identification and authentication of individuals is key to the use of biometrics. The development of an identification database, which obtains the biometrics of all individuals related to the system, is required to allow for one-to-many identification – in which an individual's presence in an existent population can be determined; to ascertain whether the individual is on a prohibited list; and to ensure that the individual is not already placed on a different identity system. The use of an identification process can also determine whether an individual has already enrolled within a system, through the comparison of pre-collected biometrics; this is considered one of the fundamental uses of the identification process. Authentication is usually undertaken through one-to-one comparisons in which the identity of the user present is confirmed. This process is completed through the use of an enrolled biometric template, which is held on a locally or centrally formed database, using a device with the sole purpose of confirming authentication [24].

C. Radio Frequency Identification (RFID) Technology

Radio frequency identification (RFID) system consists of the following three components (see "Fig. 3"):

- RFID tag or transponder
- RFID reader or transceiver with a scanning antenna
- A host computer.

An RFID reader is constructed of an antenna, transceiver and decoder, and is used to transmit regularly signals to determine whether any RFID tags are in the area. Received signals are then processed through a data processor attached to the RFID reader, which stores the data.

As Mohandes [22] highlights, an RFID tag is a microchip formed of an antenna, a wireless transducer and an encapsulating material. RFID tags can be developed in the form of tokens, coins, embedded tags, wristbands and so on.

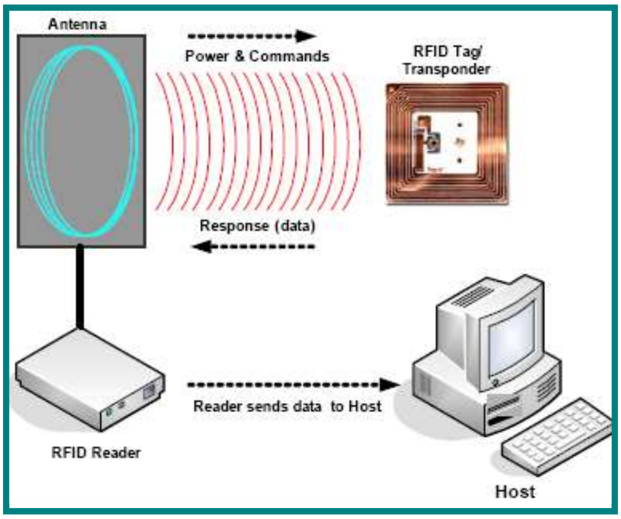

Fig. 3. A Typical RFID System [22]

D. Identification Wristband

An identification appliance, such as a wristband, headband, armband, ankle band, or leg band, has a wireless communication circuit to enable communication with a system, network, or device. The appliance may provide information about the authorized bearer: name, address, phone number, passport number, driver's license data, social security number, credit card information, fingerprint data, biometric voice characteristics, retinal characteristics, and medical data. Identification wristbands have become a convenient and effective way of identifying people without permanently marking them. A principle advantage of a wristband is that it is ultimately removable. It includes any control unit such as a microprocessor, microcontroller or digital hardware and software. The improved wristband appliance contains an RFID function of any type or frequency, operates in low and/or high frequencies, and can be read-only or permit both read and write functions [36, 38]. Wristband (or bracelet) RFIDs have various designs; normally they are light, colorful, smooth, easy to carry, and water proof. Wristband tags can be used for human identification and access control; and it is for the aforementioned reasons that fingerprint technology is used in this system (see "Fig. 4"). These wristband tags can also support data encoding, encryption options and individual process [37]. Based on these benefits, it will be used in our system - the Identification Wristband Permission to Hajj (IWPH).

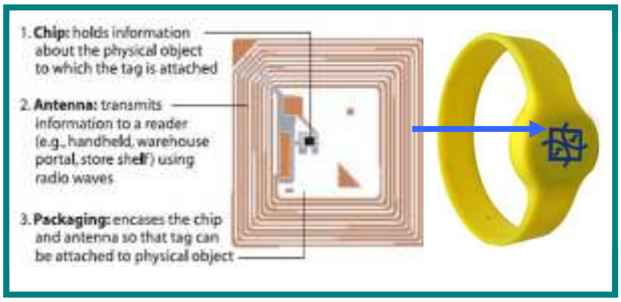
1. Chip: holds information about the physical object to which the tag is attached
2. Antenna: transmits information to a reader (e.g., handheld, warehouse portal, store shelf) using radio waves
3. Packaging: encases the chip and antenna so that tag can be attached to physical object

Fig. 4. RFID Wristband [36, 37]

E. A Hash Function

"Hash functions are mathematical computations that take in a relatively arbitrary amount of data as input and produce an output of fixed size. The output is always the same when given the same input. The inputs to a hash function are typically called messages, and the outputs are often referred to as message digests". At this time, any type of data can be defined as a message, including character strings, binary files and TCP packets. It is widely used in database indexing, compiler design, caching, password authentication, software integrity variation, error-checking, and many other applications [39]. The properties of some hash functions can be used to greatly increase the security of a system administrator's network; when implemented correctly they can verify the integrity and source of a file, network packet, or any arbitrary data [40].

III. Material and Methods

Following the methodology used in this study, the research consisted of the following stages:-

Stage 1: Biometric Cryptosystem for Hajj Permission

Securing Hajj permissions will be based on public Hajj information on IWHP (RFID Wristband), in which one biometric identification method in a central secured database will be used in the authentication. Thus, there will be a combination of cryptography (digital signature) and biometrics, known in the literature as Biometric Cryptosystem, to benefit from the strengths of both fields [22, 41]. Each pilgrim is then identified by the IWHP, which is a component of the public key infrastructure (PKI) (i.e. everybody should have a public key and private key, see "Fig. 5&6").

Fig. 5. Hajj permission before IWPH [19]

Fig. 6. Hajj permission after IWPH

Stage 2: Certification and Key Management

In order to ensure validity and security, a system will be devised for the certification and key management of IWHP. Within this system, digital signature key ownership can be held only by specific authorized permit issuers. The public key of each national body is verified through a certification authority (CA) of the National Center for Digital Certification [42]. In order to ensure the authentication of the IWHP holder, the verification key of the NCDC must be analyzed. A scheme that proffers the use of the tiny public exponent of the RSA algorithm allows the use of IWHP to enhance the authentication process [30, 43]. The Hajj Ministry is in a position to determine the validity period of the certification of the IWPH, through the restriction of the signature/private key, which is likely to be one month.

Stage 3: The Digital Signature Algorithms of IWHP

For the issuance of permits, the digital signature scheme of IWPH based on Asymmetric Cryptography is proposed to describe the authentication that confirms that identity credentials belong to the individual present. Our scheme uses one biometric identification method for our general system and consists of three algorithms: key generation, signing, and signature verifying Algorithms.

Key Generation Algorithm: A key generation algorithm produces public-private keys $(e, N)$and (d, N), where N is the product of two distinct large primes - p and q. In this phase, the following will be undertaken:

1) Compute the secret exponent$d$,$1 < d < \varphi(p, q)$, such that for Euler totient function $\varphi(p, q) = (p - 1)(q - 1)$(1) [24];
2) Compute the exponent e that is chosen from a reasonably small space for efficiency in signature verification. It is widely recognized that $e = 3$ or 2^{16+1} is good for digital signatures [30].
3) Assume the authorized party, such as the permits issuing department, owns RSA key and provides it to certify the public key (e, N) by the CA in NCDC and valid in the current epoch.
4) Once the RSA key is generated and certified, it can be used for signing off the IWPH applicant. The signature generation key (d, N) will be maintained securely.

Signing Algorithm: A signing algorithm which has given the data of pilgrim D via RFID reader and also a private key (d, N) via the host produces a signature S on the D. In this phase, the following will be undertaken:

1. IWPH hashes D to produce hash, which it then registers.
2. Asymmetric algorithm: takes as input parameters, hash, and the private key (d, N) to return the digital signature (S). The following is also undertaken:-
   a. Obtains the private key (d, N) which it then stores.
   b. Represents hash as a positive integer h.
   c. Computes $S = h^d \bmod N$ (3). S will be stored in the database via the RFID reader (see “Fig. 7”).

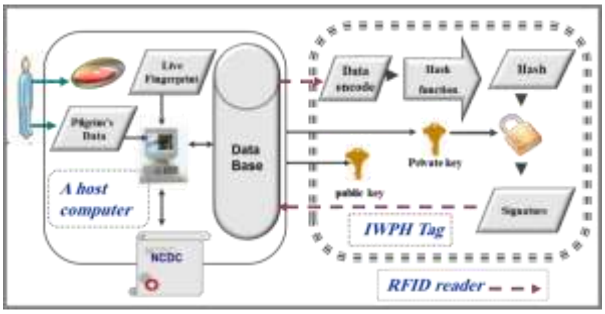

Fig. 7. The diagram showing how a digital signature is applied

Signature Verifying Algorithm: The signature verifying algorithm, which has given S, the CA public key (e, N) and the Live Finger Template (LB), produces either ‘accepts’ or ‘rejects’ for the IWPH's holder authenticity. To ensure this, the IWPH will run the following two algorithms in parallel:

1) It compares the live LB and soared B using the match method (based on RFID technology).
   a. If they match, then the digital signature will be verified.
   b. If they do not match, then the algorithm will be rejected.
2) It will request the hash by hashing D, and verify the signature S using her/his CA public key. If the matcher returns a verified flag, S will be decrypted by the Asymmetric algorithm using her/his CA public key (e, N) to output the new hash. IWPH undertakes the following:-
   a. Uses the public key (e, N) to compute the new hash $h` = S^e \bmod N$(2) extracts the hash from the representative h.
   b. Compares the hash and the new hash
      - If they match, then the wristband holder W will be verified.
      - If they do not match, then the algorithm will be rejected.
      - If the matcher returns a rejected flag, the system will reject the wristband holder (see “Fig. 8”).

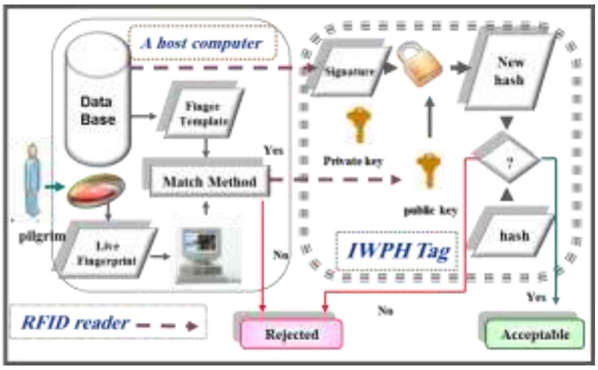

Fig. 8. The diagram showing how a digital signature is verified

IV. Analysis and Results of Proposed System

In this system, the digital signature is generated by encrypting the hash with the private key. The signature is verified by using the public key to decrypt the digital signature and to recover the original hash. The original hash is then compared to the newly generated hash, and if they match, the digital signature is verified.

- The signature algorithm is derived from a hash of the original information using ($h^d\ mod\ N$). The signature verifying algorithm will need to follow exactly the same process to derive the same hash, using ($S^e mod\ \ N$).
- Calculating ($h^d\ mod\ N$) is easy, but calculating the inverse ($S^e mod\ \ N$) is difficult, in the case of large N's. Calculating the factor N into its prime factors p and q thus becomes the easiest solution.
- The common choices for e are 3, 17 and 65537 (2^{16+1}). These are primes; they are chosen because they make the modular exponentiation operation faster. Also, having chosen e, it is simpler to test whether gcd($e, p-1$) $= 1$ and gcd($e, q-1$)$= 1$ while generating and testing the primes in algorithm 1. Values of p or q that fail this test can be rejected immediately.
- To compute the value for d, we have used the Extended Euclidean Algorithm to calculate (this is known as modular inversion).

Therefore, the proposed system satisfies the basic security services of confidentiality, authentication, integrity and non-repudiation and also provides usability features such as accuracy.

1) Confidentiality is provided in this proposed system through:
   a. The data of pilgrim is encrypted and stored in IWPH.
   b. The fingerprint is registered in a secured database.
   c. The IWPH is only authorized to access the asymmetric cryptography.
   d. The private key is maintained securely in the IWPH using the suitable protocol, where confidentiality is provided.
2) Authentication is provided by the following:
   a. Two factor authentications -something you have (IWPH) and something you are (pilgrim fingerprint).
   b. By storing the fingerprint of a pilgrim in the secured database to verify the person's identity, we can prove the ownership of the fingerprint to the pilgrim that will provide the authentication service by using the match method and the IWPH's holder's private key.
   c. The system will perform the comparison operation between the hash and the new hash to verify the IWPH's identity where there is strong authentication for the pilgrim's identity.
3) Integrity: The proposed system provides this service by using the digital signature. The IWPH will sign off the data through the use of a private key using a hash algorithm; the digital signature will then be incorporated into the data. It will be automatically alert the inspector in the following cases: if there is an invalid signature, or if the live template does not match the stored template.
4) Non-Repudiation: The proposed system supports authentication and integrity services and also provides non-repudiation services by storing the fingerprints of the pilgrim and maintaining private keys in IWPH. The holder cannot deny the ownership of the registered fingerprint, as specific rules are required to verify the identity of the registered person. The fingerprint is stored in a secured database to ensure credibility and confidence.

Accuracy: Biometric accuracy can be rated by using false-acceptance rate (FAR) or false-rejection rate (FRR) methods which focus on the system's ability to allow limited entry to authorized users. The Hajj system supports the system security requirements to achieve a high level of accuracy by adding fingerprint technology (e.g. for a high security environment, trying to achieve a low FAR and tolerating a higher FRR) [24]. The proposed IWHP satisfies the basic security services of confidentiality, authentication, integrity and non-repudiation, provides some usability features such as accuracy and is sensitive to the context of the Hajj environment.

V. Discussion

The issuance of permits controls the numbers of persons authorized to pilgrim in a more efficient and secure manner than the current system. The proposed model and system has the following attributes:

1) Two authentications are used to authenticate or verify the identity of a person to control the issuing of permits, excluding the password.
2) Wristbands are gaining popularity as the medium for private keys. These wristbands are also a point of convergence for public key certificates and associated keys because they:
   - Provide tamper-resistant storage for protecting private keys and other forms of personal information.
   - Isolate security-critical computations, involving authentication, digital signatures, and key exchange from other parts of the system that do not require such knowledge.
3) A digital signature key is a PKI solution for enabling the enhanced user identification and access controls needed to protect sensitive online information, by storing in IWPH.
4) It is certified and managed in the system by restricting the validity period of the private key.
5) Each certificate can only be used to authenticate one pilgrim as only that holder's IWPH has the corresponding and unique private key needed to complete the authentication process.
6) The RSA key is generated and used for signing hash where the security of the scheme can rely on the signature of the authorized permit-issuing.
7) The verification performance is improved by assuming the authorized party's key pairing and by allowing a tiny public exponent of the RSA

algorithm, ensuring more efficient real-time processes.

8) The framework shows that if the two hash values are same, the accept match signal is generated; therefore the inspector has the confidence that the data had been signed off by the owner of the private key and that the integrity, confidentiality, creditability, and authentication are achieved.

The proposed model and framework builds on and complements previous work on technology to support Hajj. We improve and enhance the work of Mohamed Mohandas [22] by adding PKI Authentication and using biometric technology to automatically verify the identity pilgrims. In addition, the framework is somewhat similar to Federated Identity [41], which considers authentication systems based on smart cards, where the smart cards will be issued by many organizations, and authentication must work at any location. The IWPH, however, explored a stronger authentication framework based on wristbands, fingerprints and digital signature techniques with PKI for the issuance of Hajj permissions. The suggested IWPH model potentially has wider applicability and in the first instance it could be similarly applied (i.e. issuing RFID wristband-based permissions) across holy places in Saudi Arabia. Similarly the IWPH model could be applied in other mega event situations as discussed in the introduction.

The paper of Kwon and Moon [43] explained several challenges in border control applications. They did not achieve Objectives 3and 4; however, this system will achieve all by:

- Taking high costs to process a small amount of biometric information and to issue IWPH for limited numbers of pilgrims at Hajj.
- Using fingerprints in the framework has a small-scale database across Saudi Arabia, where Biometrics remains a useful technology in small-scale applications, excluding worldwide border control applications.

Respect for Islam has ensured that selected fingerprints technology instead of the face technology will be used. Thus, there is no embarrassment to the pilgrims during the inspection.

VI. Limitation

To make the issuance of permits faster than the current system and to provide a high degree of accuracy of identification, we must perform further experiments by:

- Measuring the performance of biometric matching methods under controlled false reject rates (FRR) and false accept rates (FAR) to test the performance of the framework.
- Proving that the encryption process required is quicker than the decryption process, as the latter is performed after extracting and matching the finger features simultaneously. The reject match signal and accept match signal are more suitable to evaluate the performance of the decryption processes. Thus this can be explored by implementing the two processes and computing the complexity time of both.
- Evaluating the application of the system in real-time environments using large numbers of people.

VII. Conclusion

Event management of large international events or mega events of sporting or religious occasions is attracting increased interest from researchers. The challenges are significant in managing such events as a result of the complexities in ensuring the safety of the participants, the wider community and the smooth operation of the events. The challenges become increasingly intricate when one considers that there will be some limit to resources or capacity for the event and events can often be oversubscribed. There needs to be active management to limit access to legitimate participants and to ensure that there are adequate resources allocated. Technology clearly has a role to play in managing these mega events. The case example presented here is that of the Hajj religious festival which can attract over three million pilgrims. The paper presents a suggested technological support solution, the IWPH, which is sensitive to the context of the Hajj, reducing the need for facial recognitions systems often used in managing other large international events. The proposed solution has some generic properties that may be suitable for other events, such as the scalability, low cost and robust authentication capabilities.

The suggested IWPH model has novelty in utilizing RFID type bracelets, PKI authentication algorithms, key generation, signing, and signature verifying algorithms, and biometric information. The paper makes a contribution by identifying the specific challenges of mega events like the Hajj pilgrimage and by developing a context sensitive solution providing robust attributes to support active management of such events. The solution has generic attributes that could be applied to other such events and consequently provides a base for other researchers to explore solutions in other contexts. The proposed IWPH provides strong authentication, access control and non-repudiation for the issuance of permits for the pilgrims and the employees who work there. An initial evaluation of the attributes indicates it will be faster than the current system and be sensitive to the context of the Hajj environment. In addition, each pilgrim is identified by IWHP which allows for a protocol to be built between the Hajj ministry and NCDC to satisfy Saudi government goals. The use of a wristband can be checked to assure the identity of the pilgrim with high accuracy and to track the pilgrim. This provides a service for the pilgrims and also assists in controlling the number of pilgrims in holy places.

References

[1] Goldblatt, J. : The roots and wings of celebration (5th ed.). John Wiley & Sons (2007).

[2] Horne, J., & Manzenreiter, W. : Sports mega-events: social scientific analyses of a global phenomenon. Sociological Review, 54 (Suppl. 2), 1-187 (2006).

[3] Bahurmoz, A. M. : A strategic model for safety during the Hajj pilgrimage: an ANP application. Journal of Systems Science and Systems Engineering, 15(2), 201-216 (2006).

[4] Li, S. : Large Sporting Events and Economic Growth: Evidence from Economic Consequences of Event Infrastructure and Venues. Event Management, 17(4), 425-438 (2013).

[5] Economist. : Why would anyone want to host the Olympics?. Retrieved 12/04/2014, from http://www.economist.com/blogs/economist-explains/2013/09/economist-explains-0 (2013)

[6] Goldblatt, J. J. : Twenty-first century global event management (3rd ed.). Wiley (2002).

[7] Bowdin, G., Allen, J., O'Toole, W., Harris, R., & McDonnell, I. : Events management (3rd ed.). Routledge (2010).

[8] Memish, Z. A., Stephens, G. M., Steffen, R., & Ahmed, Q. A.: Emergence of medicine for mass gatherings: lessons from the Hajj. The Lancet infectious diseases, 12(1), 56-65 (2012).

[9] Yamin, M., & Ades, Y.: Crowd management with RFID and wireless technologies. Paper presented at the First International Conference on Networks and Communications, 2009. NETCOM'09 (2009).

[10] Tarlow, P. E. : Event risk management and safety. John Wiley & Sons (2002).

[11] ITV. : India to host the largest religious event in the world. Retrieved 12/04/2014, from http://www.itv.com/news/2013-01-13/india-to-host-the-largest-religious-event-in-the-world/ (2013)

[12] Ministry of Hajj. : Instructions Regulating Agreements Between Hajj Missions and the Ministry (2010).

[13] Eid, R.: Towards high-quality religious tourism marketing: the case of hajj service in Saudi Arabia. Tourism Analysis, 17(4), 509-522 (2012).

[14] Silvers, J. R., Bowdin, G. A., O'Toole, W. J., & Nelson, K. B. : Towards an international event management body of knowledge (EMBOK). Event Management, 9(4), 185-198 (2005).

[15] Henderson, J. C.: Religious tourism and its management: The hajj in Saudi Arabia. International Journal of Tourism Research, 13(6), 541-552 (2011).

[16] Jafari, J., & Scott, N. : Muslim world and its tourisms. Annals of Tourism Research, 44, 1–19 (2014).

[17] Mantoro, T., Jaafar, A. D., Aris, M. F. M., & Ayu, M.: Hajj locator: A hajj pilgrimage tracking framework in crowded ubiquitous environment. Paper presented at the International Conference on Multimedia Computing and Systems (ICMCS), (2011).

[18] Yamin, M.: A Framework For Improved Hajj Management And Research. Paper presented at the International Conference on Wireless Communications and Sensor Networks (2006).

[19] Tareeb News. : Find 554 Hajj permit forged 350 of them in the Asian campaign. Retrieved 12/04/2014, from http://www.tareebnews.com/news.php?action=show&id=13552 (2014)

[20] Symantec. : National PKI: The Foundation of Trust in Government Programs. White Paper (2011).

[21] Binsalleeh, H., Mohammed, N., Sandhu, P. S., Aljumah, F., & Fung, B. C. M.: Using RFID tags t12/04/2014,o improve pilgrimage management. Paper presented at the International Conference on Innovations in Information Technology, IIT'09 (2009).

[22] Mohandes, M .: An RFID-based pilgrim identification system (a pilot study). Paper presented at the 11th International Conference on Optimization of Electrical and Electronic Equipment, OPTIM 2008 (2008).

[23] Ravi, K. S., Aziz, M. A., & Ramana, B. V. : Pilgrims Tracking and Identification Using RFID Technology. Advances in Electrical Engineering Systems, 1(2), 96-105 (2012).

[24] Alliance Smart Card.: Smart Cards and Biometrics in Privacy-Sensitive Secure Personal Identification Systems: Smart Card Alliance (2002).

[25] Liu, S., & Silverman, M. : A practical guide to biometric security technology. IT Professional, 3(1), 27-32 (2001).

[26] TCMCORE. : Transport and Crowd Management workshop,Center of Research Excellence in Hajj and Omrah ,Park Hyatt Resort - Jeddah, Saudi Arabia (2010).

[27] Al-Khouri, A. M.: PKI in Government Digital Identity Management Systems. European Journal of ePractice, 4, 4-21 (2012).

[28] Bella, G., Bistarelli, S., & Martinelli, F.: Biometrics to enhance smartcard security. Paper presented at the Security Protocols (2005).

[29] Watts, J., Yu, H., & Yuan, X.: Case study: Using smart cards with pki to implement data access control for health information systems. Paper presented at Proceedings of the IEEE SoutheastCon (SoutheastCon), (2010).

[30] DI Management. : RSA Algorithm. Retrieved 9/04/2014 from http://www.di-mgt.com.au/rsa_alg.html (2002)

[31] Vacca, J. R.: Public Key Infrastructure: Building Trusted Applications and Web Services: CRC Press (2004).

[32] Weise, J.: Public key infrastructure overview. Sun Blue Prints OnLine, August (2001).

[33] Shan, L.: The PKI authentication system with the integration of biometric identification and non symmetric key technology'. Paper presented at the International Symposium on Web Information Systems and Applications (WISA'09) (2009).

[34] RSA Data Security: Understanding Public Key Infrastructure (PKI). White Paper (1999).

[35] MacGregor, W., Mehta, K., Cooper, D., & Scarfone, K.: Information Security. (2008).

[36] Mohandes, M. : A Case Study of an RFID-based System for Pilgrims Identification and Tracking. Sustainable Radio Frequency Identification Solutions, InTech, 87-104 (2010).

[37] PRLog. : RFID Wristband and Bracelet Selections. Retrieved 10/04/2014 from http://www.prlog.org/10281756-rfid-wristband-and-bracelet-selections.html (2009).

[38] Beigel, M., Mosher, W., Tuttle, J., & Wang, D.: Wearable identification appliance that communicates with a wireless communications network such as bluetooth. Google Patents (2003).

[39] RSA Laboratories. : RSA Laboratories' Frequently Asked Questions about Today's Cryptography, What is a hash function? Version 4.1, Retrieved 9/04/2014 from http://www.rsasecurity.com/rsalabs/faq/2-1-6.html (2000)

[40] Silva, J. E. : An Overview of Cryptographic Hash Functions and Their Uses. GIAC Security Essentials Practica (2003).

[41] Isode.: Federated Identity, Distributed PKI and Smart Cards (2007).

[42] NCDC. : National Centre for Digital Certification, Retrieved 9/04/2014 from http://www.ncdc.gov.sa/en/ (2013)

[43] Kwon, T., & Moon, H.: Biometric authentication for border control applications. Knowledge and Data

Engineering, IEEE Transactions on, 20(8), 1091-1096 (2008).

Authors' Profiles

Ebtehal A. Alsaggaf earned master degree in computer science at King Abdul-Aziz University, Jeddah, Saudi Arabia. She is working as lecturer at Faculty of Computing and Information Technology – Computer Science Department- King Abdul-Aziz University, Jeddah, Saudi Arabia

Dr.Omar Abdulla Batarfiis is working as assistant professor at Faculty of Computing and Information Technology – Information Technology Department- King Abdul-Aziz University, Jeddah, Saudi Arabia. His research interests include information security.

Dr.Nahla Aljojo earned a PhD in Computing at Portsmouth University, UK. She is working as assistant professor at Faculty of Computing and Information Technology – Information System department- King Abdul-Aziz University, Jeddah, Saudi Arabia. Her research interests include adaptivity in Web based educational systems and information security.

Dr.Carl Adams is working as Principal Lecturer in Computing at Portsmouth University, UK. He is an active researcher in the School of Computing engaged in investigating information systems, mobile information systems and technologies and the impact of technology on people, organisations and society.

How to cite this paper: Ebtehal Alsaggaf, Omar Batarfi, Nahla Aljojo, Carl Adams,"Secure Hajj Permission Based on Identifiable Pilgrim's Information", International Journal of Information Technology and Computer Science(IJITCS), vol.7, no.5, pp.67-76, 2015. DOI: 10.5815/ijitcs.2015.05.10